Dear Sirs,

I am writing to notify you of a recent data breach within Ealing Council.

Please find attached our notification form and further details relating to this incident. .

Yours faithfully

FOIA s.44 - Prohibition on disclosure
Corporate Information Governance Manager
020 8825 5512

Data protection breach notification form

This form is to be used when data controllers wish to report a breach of the Data Protection Act to the ICO. It should not take more than 15 minutes to complete.

If you are unsure whether it is appropriate to report an incident, you should read the following guidance before completing the form: Notification of Data Security Breaches to the Information Commissioner's Office.

Please provide as much information as possible and ensure that all mandatory (*) fields are completed. If you don't know the answer, or you are waiting on completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident reports.

In the wake of a data protection breach, swift containment and recovery of the situation is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form.

1. Organisation details

(a) * What is the name of your organisation – is it the data controller in respect of this breach?

London Borough of Ealing

(b) Please provide the data controller's registration number. Search the online Data Protection Public Register.

Registration reference: **Z5696801**

(c) * Who should we contact if we require further details concerning the incident?

FOIA s.44 - Prohibition on disclosure

Corporate Information Governance Manager
Ealing Council
Perceval House
14-16 New Broadway
Ealing
W5 4HL

Email – FOIA s.44 - Prohibition on disclosure
Telephone: FOIA s.44 - Prohibition on disclosure

2: Details of the data protection breach

a) Please describe the incident in as much detail as possible.

A data breach has taken place on FOIA s.44 - Prohibition on disclosure resulting in confidential information contained in a number of court related documents being lost in public.

b) When did the incident happen?

FOIA s.44 - Prohibition on disclosure

c) How did the incident happen?

FOIA s.44 - Prohibition on disclosure

The Social worker left Court and put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents and drove the same route back, however was unable to locate the envelope containing the documents. She also returned to the Court to establish if the documents had been handed in from the car park both the same day and the following morning.

d) If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

A Data Breach incident meeting was convened on FOIA s.44 - Prohibition on disclosure to discuss containment and recovery of the incident. Time was given to allow for further enquiries to be made to try and recover the documents from the area surrounding the court and also to allow for the documents to be posted back to Ealing Council. A follow-up data breach meeting was convened on FOIA s.44 - Prohibition on disclosure whereby it was reported the documents had not been recovered leading to the decision to notify.

e) What measures did the organisation have in place to prevent an incident of this nature occurring?

Ealing Council has Paper Records policy to provide guidance on taking papers out of the office.

f) Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented.

Data Protection Policy - current version implemented in 2012 reviewed in January 2016.

Paper Records Policy – created 2012 – due to be reviewed 2016

3: Personal data placed at risk

a) What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

FOIA s.44 - Prohibition on disclosure

[redacted]

FOIA s.44 - Prohibition on disclosure

[redacted]

c) Are the affected individuals aware that the incident has occurred?

Following the data breach meeting on [redacted] the following notifications took place

Immediate notification by telephone [redacted]

[redacted]

Notification by letter [redacted]

[redacted]

d) What are the potential consequences and adverse effects on those individuals?

Potential risk of contact from unknown third party and uninvited approaches with the young people.

e) Have any affected individuals complained to the organisation about the incident?

Not at the time of notification

4:Containment and recovery

a) Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

We have notified the individuals concerned both by phone and letter. Please see attached copies of letters sent.

b) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

No, at the time of notification the data has not been recovered

c) What steps has your organisation taken to prevent a recurrence of this incident?

We have a Paper Records policy for staff to adhere to and it is unfortunate that in this instance this was not followed.

Staff will be reminded of the need to comply with the Paper Records Handling policy if they are taking documents out of the office.

5: Training and guidance

a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

When new staff join the organisation data protection forms part of their induction course. They are required to complete our e-learn Data Protection training module.
The data protection team are fully qualified FOIA s.44 - Prohibition on disclosure and provide training to service areas across the organisation.

The Data Protection policy has recently been reviewed and disseminated to all staff.

All staff within the Children's directorate has received a briefing note reminding them of their obligations with regard to handling personal and sensitive data.

b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

When new staff join the organisation data protection forms part of their induction course. They are required to complete our e-learn Data Protection training module and have to undergo training which incorporates elements of data protection before they are given access to the social care case management system.

The Data Protection Team also regularly attends service area meetings to talk about data protection issues.

All staff within the service area will be requested to revisit the on-line data protection course.

c) As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the

incident you are reporting? If so, please provide any extracts relevant to this incident here.

Ealing council has a Paper Records Policy- please see relevant extracts below:-

Where personal or other confidential data contained within paper records/hard copy material is taken off-site and is in transit from one location to another, it should be transported in a way that mitigates against the risks of theft or loss.

Best practice guidance

If you have determined that it is necessary to take paper records/hard-copy material off-site, there are many practical actions you can take to minimise the risk of data loss. For example;

- *don't carry paper records/hard-copy materials 'loosely' as this increased the risk of dropping or losing them, or that they come loose from the rest of the file;*
- *don't carry paper records/hard-copy material in the same bag as electronic device (lap-top) or in any bag containing valuables, as these are often the primary target for thieves;*
- *ensure paper records/hard-copy material are not in transit for any longer than is necessary, and they are delivered to their destination at the earliest opportunity;*
- *don't leave bags or cases containing paper files in the car.*
- *when travelling on public transport keep you bag/case containing paper records/files/hard-copy material close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of theft or the misplacement of the item*
- *ensure paper records/hard copy materials are not away from the office for longer than is necessary and return them as soon as possible.*

6: Previous contact with the ICO

a) Have you reported any previous incidents to the ICO in the last two years?

No

b) If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

N/A

7: Miscellaneous

a) Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details.

No

b) Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

No

c) Have you informed any other regulatory bodies about this incident? If so, please provide details.

No

d) Has there been any media coverage of the incident? If so, please provide details of this.

No

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on **0303 123 1113** or **01625 545745** (operates 9am to 5pm Monday to Friday)

Ealing Council

www.ealing.gov.uk

PRIVATE AND CONFIDENTIAL

Ealing Council
Ealing Council
Perceval House 3:SE
14-16 Uxbridge Road
London W5 2HL
Tel: (020) 8825 5000

Your Ref	My Ref	Date	Please ask for	Direct line/ext.
		15/01/2025	FOIA s.44 - Prohibition on disclosure	

Dear ,

FOIA s.44 - Prohibition on disclosure

I am writing to advise you that information about this matter held by Ealing Council was unfortunately compromised recently.

This incident occurred because the Social Worker inadvertently forgot to take the documents with FOIA s.44 - Prohibition on disclosure
Please be advised that the Council has tried to do what we can to recover the documents that have been lost. FOIA s.44 - Prohibition on disclosure
At present, these documents have not been recovered.

The documents lost include the following:-

FOIA s.44 - Prohibition on disclosure

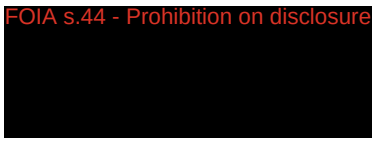
Ealing Council works to help and support adults, children and young people every day and we take these duties extremely seriously. I am very sorry that we have on this occasion, failed to meet our own high standards and I would like to offer you my sincere apologies for this matter.

I do understand this will be of concern to you and I appreciate that you may wish to discuss this further. The team manager, FOIA s.44 - Prohibition on disclosure, within our Social Care department

is available to answer any queries that you may have in respect of the information that was compromised. If you wish to speak with her, her direct line is 020 8825 6293

Finally, once again please accept my apologies for this matter and if I can be of any assistance to you please do not hesitate to contact me.

Yours sincerely



Corporate Information Governance Manager

22 February 2016

Case Reference Number COM0617270

Dear FOIA s.44 - Prohibition on disclosure

Thank you for your email of date 18 February 2016..

You have notified us about a security breach concerning the loss of documents containing details of a family and their children.

The information that you have provided has been forwarded to our Enforcement Department, who on consideration of this information will contact you in due course.

Should you wish to contact us or provide any further documentation in relation to this incident please be sure to quote the above reference number.

You can forward the additional information to us by either replying to this email, being careful not to amend the information in the 'subject' field. Alternatively, if you prefer to send in hard copies, please address them to: The Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

We would recommend that you read the guidance on our website 'Information security (Principle 7) '

If, in the meantime we can be of any further assistance please contact our Helpline on 0303 123 1113.

Yours sincerely

Sarah Elias
Case Officer
On behalf of the Enforcement Department

Dear Colleague,

This is a notification of a data loss incident which has been entered on the Information Governance Toolkit which has been deemed as reportable to the Information Commissioner's Office. Please find details of the incident in the attachment to this email.

No previous IG SIRI Level 2 Incidents have been reported by this organisation.

This information is current at the time of notification and reported by Michael Russell, russellm@ealing.gov.uk, 020 8825 8185

IG Incident Reporting Tool.

IG Incident - 04/03/2016 16:21

Incident Subject Details

ID:	**IGI/5236**
Cyber Security SIRI:	No
IG SIRI:	Yes
Clinical Safety Aspect:	No

General Details

Status:	Open
Source:	Direct
Date Of Incident:	04/02/2016
Local SIRI ID:	
Breach Type:	Lost or stolen paperwork
Summary of Incident:	A social worker put an envelope containing confidential documents on top of her car after attending court and then drove off.
Details of Incident:	Incident separately reported to the ICO.

FOIA s.44 - Prohibition on disclosure

When she left court, she put an envelope containing confidential documents on the top of her car and then drove off.

When she got home she realised that she did not have the documents and drove the same route back, however was unable to locate the envelope containing the documents. She also returned to the court to establish if the documents had been handed in from the car park both the same day and the following morning.

FOIA s.44 - Prohibition on disclosure

Organisation Details

Code:	722
Name:	LONDON BOROUGH OF EALING
Type:	Local Authority
Role:	Other

Severity Details

IG SIRI Level:	**Level 2 - Confirmed IG SIRI that must be reported to ICO & DH**
Scale of Incident:	Information about 11-50 individuals
Sensitivity Factors:	*Sensitivity factors assigned as below:*

Low Sensitivity Factors

None assigned

High Sensitivity Factors:

- Detailed information at risk e.g. clinical/care case notes, social care notes
- High risk confidential information

ICO Estimated Detriment: **High**

Data Details

Data:

FOIA s.44 - Prohibition on disclosure

	FOIA s.44 - Prohibition on disclosure
Format:	Paper
Volume:	FOIA s.44 - Prohibition on disclosu
Encrypted:	Not Applicable

Post Incident Details

Media Aware:	No
Media Notes:	
Data Subjects or Users Informed:	Yes
Police Informed:	No
Actions Taken:	A data breach incident meeting was convened on the FOIA s.44 - Prohibition on disclosure to discuss containment of the incident and recovery of the documents. Time was given to allow for further enquiries to be made to try and recover the documents from the area surrounding the court and also to allow for the documents to be posted back to Ealing Council. A follow-up data breach meeting was convened on the FOIA s.44 - Prohibition on disclosure whereby it was reported that the documents had not been recovered, leading to the decision to notify.
Lessons Learned:	FOIA s.44 - Prohibition on disclosure All staff within the Children's Directorate have received a briefing note reminding them of their obligations with regard to handling personal and sensitive data. When new staff join the organisation, data protection forms part of their induction course. They are required to complete our e-learn data protection training module and have to undergo training which incorporates elements of data protection before they are given access to the social care case management system. All staff within the service area will be requested to revisit the on-line data protection course. Staff will be reminded of the need to comply with the Paper Records Handling Policy if they are taking documents out of the office.

Information Commissioner's Office (ICO) Information

ICO Informed:	
ICO Action Date:	
ICO Action:	Not Known

Authorisation

Notify:	Now
Level 2 SIRI Notification Approved:	Yes
Approver Name:	FOIA s.44 - Prohibition on
FOIA s.44 - Prohibition on disclos	Corporate Information Governance Manager

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

The Information Commissioner's powers

There are a number of powers available to the Information Commissioner's Office (ICO) in respect of breaches of the Data Protection Act 1998 (the DPA).

Our powers are not mutually exclusive. We will use them in combination where justified by the circumstances.

The main options are to:

- provide practical **advice** to organisations on how they should handle data protection matters;
- require organisations to produce **improvement plans**, setting how out they intend to improve compliance;
- issue **undertakings** committing an organisation to a particular course of action in order to improve its compliance;
- serve **enforcement notices** where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct **consensual assessments** (audits) to check organisations are complying;
- serve **assessment notices** to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- issue **monetary penalty notices** requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act occurring on or after 6 April 2010;
- **prosecute** those who commit criminal offences under the Act. In Scotland, where the ICO is satisfied that there are grounds for a prosecution, it will make a report to the Procurator Fiscal to make a determination whether or not to prosecute.

Information about action we have taken can be found on our website:

https://ico.org.uk/action-weve-taken/

INFORMATION COMMISSIONER'S OFFICE
INVESTIGATION PLAN

Case reference:	**COM0617270** **IGI/5236**	**Basic Case Details and DPA Principles:**	FOIA s.44 - Prohibition on disclosure [redacted] left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents which have not been recovered. **27? DS (incl. 14 children). Principle 7**
Data Controller:	London Borough of Ealing	**Notification Reference:**	**Z5696801**
Date received by ICO:	18 February 2016	**Date referred to Enforcement:**	22 February 2016
Date allocated:	7 March 2016	**Case Officer/ Investigation Team:**	FOIA s.40(2) - Personal data that doesn't fall under [redacted] CivE Team 1

Priority *As set out on risk assessment*	Low Medium High	Completion ☐ 42 days ☒ 63 days ☐ 112 days	Any other information relevant to the priority of this case:
Media Interest	Yes No Unknown	☐ ☒ ☐	Details: At the time of notification.
Equality and Diversity Issues	Yes No Unknown	☐ ☐ ☒	Details:
International case?	Yes No	☐ ☒	Details:

	Unknown	☐	Is a GPEN alert required?

Case Details

Incident

FOIA s.44 - Prohibition on disclosure [redacted]

The Social worker left Court and put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents and drove the same route back, however was unable to locate the envelope containing the documents. She also returned to the Court to establish if the documents had been handed in from the car park both the same day and the following morning.

FOIA s.44 - Prohibition on disclosure [redacted]

FOIA s.44 - Prohibition on disclosure [redacted]

19 Data Subjects affected.

A Data Breach incident meeting was convened on FOIA s.44 - Prohibition on disclosure to discuss containment and recovery of the incident. Time was given to allow for further enquiries to be made to try and recover the documents from the area surrounding the court and also to allow for the documents to be posted back to Ealing Council. A follow-up data breach meeting was convened on FOIA s.44 - Prohibition on disclosure whereby it was reported the documents had not been recovered leading to the decision to notify.

Policies/ Procedures

Data Protection Policy - current version implemented in 2012 reviewed in January 2016.

Paper Records Policy – created 2012 – due to be reviewed 2016

Ealing council has a Paper Records Policy- please see relevant extracts below:-

Where personal or other confidential data contained within paper records/hard copy material is taken off-site and is in transit from one location to another, it should be transported in a way that mitigates against the risks of theft or loss.

Best practice guidance

If you have determined that it is necessary to take paper records/hard-copy material off-site, there are many practical actions you can take to minimise the risk of data loss. For example;

- *don't carry paper records/hard-copy materials 'loosely' as this increased the risk of dropping or losing them, or that they come loose from the rest of the file;*
- *don't carry paper records/hard-copy material in the same bag as electronic device (lap-top) or in any bag containing valuables, as these are often the primary target for thieves;*
- *ensure paper records/hard-copy material are not in transit for any longer than is necessary, and they are delivered to their destination at the earliest opportunity;*
- *don't leave bags or cases containing paper files in the car.*
- *when travelling on public transport keep you bag/case containing paper records/files/hard-copy material close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of theft or the misplacement of the item*

ensure paper records/hard copy materials are not away from the office for longer than is necessary and return them as soon as possible.

Training

a) As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

When new staff join the organisation data protection forms part of their induction course. They are required to complete our e-learn Data Protection training module. The data protection team are fully qualified FOIA s.44 - Prohibition on disclosure and provide training to service areas across the organisation.

The Data Protection policy has recently been reviewed and disseminated to all staff.

All staff within the Children's directorate has received a briefing note reminding them of their obligations with regard to handling personal and sensitive data.

b) Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

When new staff join the organisation data protection forms part of their induction course. They are required to complete our e-learn Data Protection training module and have to undergo training which incorporates elements of data protection before they are given access to the social care case management system.

The Data Protection Team also regularly attends service area meetings to talk about data protection issues.

All staff within the service area will be requested to revisit the on-line data protection course.

Policy specific to this incident: See extract above under **Policy/Procedure**

Remedial Action

a) Has the organisation taken any action to minimise/mitigate the effect on the affected individuals? If so, please provide details.

We have notified the individuals concerned both by phone and letter. Please see attached copies of letters sent.

b) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.

No, at the time of notification the data has not been recovered

c) What steps has your organisation taken to prevent a recurrence of this incident?

We have a Paper Records policy for staff to adhere to and it is unfortunate that in this instance this was not followed.

Staff will be reminded of the need to comply with the Paper Records Handling policy if they are taking documents out of the office

ICO Involvement with DC

To include a list of cases dealt with by the ICO over the past two years, including case reference, current status, similarity of breach, whether further action was/ is required (formal or informal) and a description of the case.

Please also include any relevant notes/ extracts from the Intelligence Log and a description of any Good Practice involvement with the DC including the type of audit and the outcomes/ recommendations.

Audit carried out 13-15 May 2013 and Action Plan 20140120. Areas for improvement (4.2 second bullet point) and audit item a13 identified the need to improve/implement refresher DP training. The follow-up in 2014 suggested that this was one of the outstanding actions that should be prioritised for completion. (*No further correspondence confirming completion found*)

For Info: Audit items a27 to a29 covered 'manual records taken off site' which is mandated by a 'Paper Records Secure Handling and Transit Policy'

No other ICO involvement in the last two years.

For Info: MPN issued 0n 04/02/11 as a result of a breach involving the theft of two unencrypted laptops containing sensitive personal data, (ENF0370035).

Initial Assessment

Case Officer Recommendations

Name: [redacted]
Date: 16 March 2016

Comments: Further information required from DC to assist assessment, with particular reference to refresher training and paper records handling.

Team Manager Approval

Name: Laura Middleton

Date: 23 March 2016

Comments: Approved subject to minor amendments to questions, as discussed on 23/03/16. Agree that a separate question should be asked about the potential for detriment to the data subjects if the data falls into the wrong hands (in line with [redacted] email of 21 March, as recorded on CMEH).

INVESTIGATION PLAN

Action Summary

Milestone	Date
IP agreed by Team Manager (where applicable)	23 March 2016
Team Manager comments on initial lines of enquiry (where applicable)	
Initial enquiries sent/ response due	24 March 2016 due 3 May 2016
Initial Review	7 June 2016
Additional enquiries sent/ response due	
Meetings/ Interviews	
Final IP Review/ Recommendation	

Pre-Meet/ Recommendation	

Initial Enquiries

Delete/amend as appropriate

NB References made below (eg 4(f)) relate to responses contained in the council's original breach notification unless stated otherwise.

Facts

1. Q. Have the documents been recovered to date? If so, please state when. If not, please state what, if anything, the council is doing to recover the documents.

   A. No, the documents have not been recovered despite the several avenues mentioned in the notification to recover them. The Court concerned is aware the documents have been lost and we have been advised that they will contact us in the event they are handed in to the Court Office. We do not consider there to any further avenue to explore but are willing to do so if one is notified.

2. Q. Please provide a redacted copy of the type of data compromised in this incident and a sample of the most sensitive information.

   A. Please be advised that our legal department have looked into the Family Procedure Rules, it appears that there are no provisions that allow the Local Authority to communicate the information in the Statement and Care Plan to the ICO without the permission of the Court.
   They have written to the Court to request the approval of the Judge to the release of these documents and they will follow once the approval of the Court has been obtained. If we are not given approval to release these documents I will advise you accordingly.

3. FOIA s.44 - Prohibition on disclosure [redacted]

4. Q. Please provide a copy of any internal security incident report produced in connection with this incident.

   A. Please find attached.

5. Q. Is there any evidence to date that the personal data involved in this

incident has been inappropriately accessed / processed? If so, please provide details.

A. No, we do not have any evidence to date that the personal data has been inappropriately accessed or processed.

6. Q. Were the documents lost in this incident the only copies available? If so, please detail what effect, if any, the loss had on the care proceedings.

FOIA s.44 - Prohibition on disclosure is the only hand written document as advised in the Data Breach Report (page 3) A handwritten document had to be prepared at the last minute because the FOIA s.44 - Prohibition on disclosure

7. Q. Is there a possible safeguarding risk the children involved may be exposed to from the father or other third parties if the data were to fall into the wrong hands? Similarly, have any possible risks to the wife or foster parents been identified? If such risks have been identified have any mitigation measures been taken?

FOIA s.44 - Prohibition on disclosure Since the immediate notification of the affected subjects with named contact personnel for them and their counsel to contact in the event of experiencing any threat and the passage of time. At a follow up meeting on 4th April 2016, which was attended by the Interim Director of Children and Families, Assistant Director of Children and Families, the council's Caldicott Guardian, representatives from Data Protection and the Legal section it was considered that the risk should be now rated as 'low'.

Necessity

8. Q. Was it necessary to transport this amount of data for the purposes of this court attendance? If so, was it necessary that all data transported be in paper form?

A. It was considered necessary to have the information that was taken to court. This was an application for an FOIA s.44 - Prohibition on disclosure and it was felt that we needed sufficient evidence to support our application. An FOIA s.44 - Prohibition

The WIFI capability at the court is known and accepted to be problematic and has caused difficulties in the past. The Court acknowledges this. In

the circumstances, it was felt that taking physical papers would ensure all the information necessary for the hearing was available to the Social Worker without any issues of connectivity.

9. Q. Please explain why the data was transported in an envelope rather than in a secure case/bag or similar. Does the council require employees to use a secure case/bag when transporting personal data outside of council premises? Does the council provide such bags to employees? If so, please provide details of how employees are made aware of this. (This may be covered, in part, by 10. Below).

A. The corporate Paper Records Handling Policy gives clear guidance in respect of handling data outside of the office. It advises that staff should not carry paper records/hard-copy materials 'loosely' as this increases the risk of dropping or losing them, or that they come loose from the rest of the file.
Lockable bags had previously been provided by the service area but it is clear on this occasion that the policy was not adhered to.

The Paper Records Handling Policy advises that :-

Managers must have proper approval procedures and controls in place within their teams to ensure that personal data or other confidential data contained in paper records/hard-copy material is only taken off-site:-

I. when it is necessary, rather than merely convenient, to achieve a specific task;
II. for the minimum time necessary to achieve that task, and
III. in circumstances where removal is limited to the minimum amount of information necessary to achieve that task.

How managers implement the necessary arrangements and monitor compliance with this policy is for them to decide, taking account of the particular requirements of the services that their teams deliver. However, in the event that a team, for which they are responsible, suffers a loss of personal or other confidential data contained in paper records/hard-copy material taken off-site, they will need to be able to satisfactorily demonstrate that they had ensured (i) proper approval procedures and controls were in place and (ii) the procedures and controls were adhered to through adequate and appropriate checks and considerations prior to the removal in question.

Policies

10. Q. Please provide full copies of the current Data Protection Policy and Paper Records Policy detailed in 2(f). Also any other written policy or procedure relevant to the specific circumstances of this breach and describe any relevant policy or procedure which is not documented.
A. Please find attached.

11. Q. From the audit carried out by the ICO 13-15 May 2013 mention is made in the audit report (item a27) of a 'Paper Records Secure Handling and Transit Policy'. If this is different to the policy referred to in 9. above and is extant, please forward a full copy of this procedure.
    A. Please find attached.

12. Q. Please describe how you bring these policies to your employees' attention.

    A. All new staff receive data protection training as part of their induction. All staff within the Children's Directorate are required to complete the online Data Protection training module. The data protection team provides training at the induction day for new starters within Children's services. Before staff are allowed to use the case management system, they are required to attend a training course which includes data protection awareness.
    Council policies are communicated to all new staff during their induction and are accessible on the intranet. Employee contracts also include the policies to be confirmed as read and understood with their line manager. In addition, all new starters must complete the online data protection module. The data protection team provides focused training to the organisation throughout the year.

13. Q. Does the council have any procedures in place to track which paper records have been removed from the office, by whom and for what purpose? If so, please describe or forward relevant sections.

    A. The corporate Paper Records Secure Handling and Transit Policy states:

    1.1 Principles to be adopted:

    1. There is a general presumption against taking off-site personal or other confidential data contained within paper records/hard copy material.
    2. Personal or other confidential data contained within paper records/hard copy material should only be taken off-site when it is a necessity and not a convenience.
    3. Line management approval must be obtained before personal or other confidential data contained within paper records/hard copy material is taken off-site. This approval request must provide details of the personal or other confidential data proposed to be taken off-site and the necessity for doing so and the relevant times (see 2.2).
    4. Where personal or other confidential data contained within paper records/ hard copy material is taken off-site it should be kept to a minimum both in terms of content and duration.
    5. Whilst off-site and temporarily in the home of an employee (or other person covered by the policy), paper records/hard copy material containing personal or other confidential data, that is not being actively worked upon, must be kept secure and separate from any valuable items such as laptops.
    6. Where personal or other confidential data contained within paper records/hard copy material is taken off-site and is in transit from one location to another, it should be transported in a way that mitigates against the risks of theft or loss.

14. Q. Do you consider the employee involved to have breached any of the organisation's policies or procedures? If so which policies or procedures? Please inform us of the disciplinary action taken, if any, in relation to the employee involved in this incident.

A. We do consider that the employee breached the requirements of the Paper Handling Policy as described above and also the Data Protection Policy which states the following :-

Employee & Member Responsibility

All Council personnel are personally responsible and accountable for ensuring compliance with the principles of the Act and that their use and handling of personal data is in accordance with the purpose(s) the Council have notified to the Information Commissioner. Adherence to the Act forms part of Council's Code of Conduct and contract of employment.

Please be advised that the employee has subsequently resigned from her position in the organisation.

Training and Disciplinary

15. Q. I note from the ICO audit issued in June 2013 that the council agreed to develop mandatory data protection refresher training (recommendation a13). Please confirm whether the council now requires employees to complete mandatory data protection refresher training. If refresher training is required how frequently does this training occur? Please provide details as to the measures you had in place to ensure that all staff attend any mandatory refresher training. Also, please provide up-to-date statistics regarding completion of training.

A. All staff within Children's services have been asked to complete the online data protection training. This will be required to be completed yearly. The Corporate Data Protection Policy has been sent to all staff via Metacompliance and will be sent out annually to remind staff of their obligations.

16. Q. Can you confirm that the employee involved in this incident received the above mentioned data protection training? If so, when did they last receive this training prior to this incident?

A. I am advised that the employee undertook data protection training in 2014 and would have been requested to undertake the e learning data protection training.

17. Q. Similarly, a9 from the audit report: "LBE are currently trialling 'MetaCompliance' policy management software" and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

A. Metacompliance has been successfully implemented within the organisation. A programme of disseminating policies is in place. The Data Protection Policy has been sent to all staff. I will forward separate to this email the statistics regarding training.

(Additional info rec'd 06.05.16):
I have now been provided with further details regarding this and can advise you that since the beginning of 2016, there is a programme to review Information Governance policies and send them out by Metacompliance to all staff in the organisation. To date, we have reviewed the Acceptable Use Policy, Data Protection Policy and these have been sent out to all staff. The acceptance of these policies has been 100%, with the exception of staff who have not logged into the system due to long term absence.
The Information Security Policy is due to be sent out in the next two weeks and the Paper Handling Policy is currently out for review.

Remedial Measures

18. Q. In the light of the response given in 4(c), has the proposed action to minimise the possibility of a repeat of such an incident been completed? How was this action carried out and by what means was this verified/recorded?

A. The management investigation that took place identified gaps in the procedure of taking paper records out of the office. Recommendations have been made as part of a management investigation and include:

- Advice and guidance contained in the 'Paper Records Secure Handling and Transit Policy' will be updated and reviewed to ensure that it reflects social work practice and requirements. Details of the requirements should be widely circulated within social care and a link created in tri-x. Workers have been reminded of the principles of secure paper handling in the interim.
- Specific guidance to be given to workers regarding the storage of confidential information at home. It should be made clear that, unless agreed storage is available, this is an exceptional circumstance. Documentation should be destroyed using council confidential waste facilities as soon as possible. A formal process for the provision of lockable home storage should be devised.
- Each area office should have lockable cases available for workers who are required to transport papers out of the office. These should be kept securely and usage appropriately controlled.
- Consideration to be given to providing social workers from localities teams with access to mobile working devices when attending court, in a similar way to that provided to the court team.
- Roles and responsibilities for printing and transporting documents required as part of the court bundle should be clarified and confirmed with Legal. The outcome should be cascaded to social work teams.
- All Social Care staff that has not yet completed e learning modules: Data Protection & Information Sharing and Confidentiality (Social Care), are required to do so as soon as possible.

19. Q. Has the organisation put in place any other containment or safeguarding measures other than those detailed in the breach notification

A. The organisation considers that the containment and safeguarding

measures are sufficient in the circumstances and no further containment and safeguarding measures have been put in place.

20. Q. As a result of this incident, did the organisation consider whether any other sensitive personal data held by your organisation may be exposed to similar vulnerabilities? If so, what steps were taken to address this?

A. The Paper Records Handling policy is being reviewed by all directorates with a view to identifying any possible vulnerability. Consideration is being given to adopting the Legal Team's procedure for taking information to court in the social care departments. This involves transporting documents in accordance with the Paper records Secure Handling and Transit Policy. The Legal Team are currently in advanced stages of investigating electronic bundling which provides for a secure cloud based system to share information with the Court and other parties.

Miscellaneous

21. Q. Please forward a copy of the notification letter (8 February 2016) detailed in your response to 3(c).
A. Please find attached.

22. Q. Since the notification, has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

A. No, we have not received a formal complaint from any individual affected by this breach.

23. Q. Since the notification, has there been any media coverage of the incident? If so, please provide details.

A. No, there has not been any media coverage of this incident.

24. Q. If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

A. As responded to question 18., the corporate Paper Handling and Transit Policy is being reviewed and updated to reflect the specific needs of social care services.
Once agreed, the policy will be actively communicated as part of data protection training at induction days and become standing agenda items for team meetings.
The already mandatory online data protection training has been asked to be completed as a refresher by social care staff and will be monitored to ensure compliance. All staff in the Social Care and Education Legal team has undertaken an e-learning module in relation to data protection.

Advice required

Technology – N/A

Legal – N/A
Strategic Liaison – N/A
Investigations – N/A
Policy – N/A

Explain scope of advice to be sought:

Other Matters

Any further relevant information to be included here

Further Enquiries

5 July 2016:

1. Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

   Please see attached for your reference.

2. With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

   In this incident the procedure detailed in the Paper Records Secure Handling and Transit Policy was not followed and therefore there is no approval request to provide.

3. From the LBE Data Security Breach Report (05.02.16) Summary of Findings, final point "Legal Officers feedback suggests this was the first experience of the Social Workers giving evidence in court and it was a challenging day for her." : As this was the Social Worker's first experience of giving evidence in court, what, if any, additional management support/guidance was given to the Social Worker? Had the Social Worker been given any specific training with respect to this task? Had the Social Worker been given an opportunity to shadow a more experienced colleague in this kind of situation prior to the incident?

   When the social worker first started at Ealing, her line manager had several discussions with her about the importance of ensuring that documents were kept securely.

   FOIA s.44 - Prohibition on disclosure [redacted]

Finally, she was offered additional management support leading up to the Court hearing by her supervisor. They discussed how court works, the roles of the various people involved, where she would be standing/sitting, about giving evidence, how to answer questions, who to address answers to, what she can do if she needs more time to think etc. The same line manager also attended Court with her and was able to give instruction or clarify casework decisions. FOIA s.44 - Prohibition on disclosure [redacted]

4. What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

   RECEIVED: 19.08.16

   All new social care staff are required to complete the online data protection e-learning module in order to gain access to the social care line of business system. In addition Data Protection is an item on the Adults and Children's induction programme.

   The Council has a number of social workers employed on a locum basis, as is the case for many local authorities, who do not form part of the corporate HR system to track online courses. In Ealing, locums make up 27% of the Children Services and have been informed of the online refresher training programme, however, these are not captured in the statistic of a 68% completion rate of permanent staff so far. This is not to say that locums have not completed the refresher training only that our HR systems are not able to capture it.

   We are working towards 100% by the end of the year and delivering team-based refresher training sessions to include locum staff in the recording process.

5. What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

   Staff within the Social Care directorate are required to complete the e-learn Data Protection training before they attend their line of business (FWi) system training. They need to provide their certificate to confirm they have completed the e-learn Data Protection course to their manager and the FWi trainers.

   In addition, we currently perform quarterly checks on who has completed the programme using Itrent and eLearn (Corporate systems).

   We also send our Data Protection policy to all staff via Metacompliance annually to remind them of their responsibilities.

Further Issues to Determine/ Evidence to Collect

Interviews/ Meetings

N/A

Additional Enquiries

Advice required

Technology – N/A
Legal – N/A
Strategic Liaison – N/A
Investigations – N/A
Policy – N/A

Explain scope of advice to be sought:

Case Analysis and Recommendations

Seriousness of the breach

FOIA s.44 - Prohibition on disclosure [redacted]

There were two original documents in the court bundle of which no copies existed:
FOIA s.44 - Prohibition on disclosure [redacted]

FOIA s.44 - Prohibition on disclosure [redacted]

Detriment

FOIA s.44 - Prohibition on disclosure [redacted]

Policies

Both the data protection policy and the Paper Records Secure Handling and Transit Policy make clear the responsibilities of employees to maintain data security. The paper records policy also make clear the procedure to follow when removing documents from the office by both the person removing such documents and the manager(s) responsible.

Training

Mandatory data protection is carried out as part of the induction training course and has to be completed before gaining access to the social care case management system.

In addition, staff within the Social Care directorate are required to complete the e-learn Data Protection training before they attend their line of business (FWi) system training. They need to provide their certificate to confirm they have completed the e-learn Data Protection course to their manager and the FWi trainers.

Quarterly checks are performed on who has completed the programme using Itrent and eLearn (Corporate systems). The Data Protection policy is also sent to all staff via Metacompliance annually to remind them of their responsibilities.

On-line data protection refresher training is required to be completed annually.

The current completion rate for refresher training of permanent staff is 68%. However, LBE make use of locums who make up 27% of the Children Services. They are informed of the on-line data protection refresher programme but are not included in the 68% completion figure.

LBE are working towards 100% completion by the end of the year. They are

delivering team-based refresher training sessions to include locum staff in the recording process.

FOIA s.44 - Prohibition on disclosure [redacted]

Update on ICO involvement with DC

Case Officer Recommendations

- ☐ Civil Monetary Penalty Notice
- ☐ Enforcement Notice
- ☐ Undertaking
- ☐ Information Notice
- ☐ Audit – consensual
- ☐ Audit - compulsory
- ☒ Informal resolution / No Further Action
- ☒ Other action – Improvement Plan

Please provide a brief supporting paragraph, explaining why you consider the above recommendation to be the appropriate course of action, and highlighting relevant criteria in the ICO's Data Protection Regulatory Action Policy. You should also address any evidential issues which remain after your investigation:

Although I am stating informal action with an improvement plan as a recommendation, I was thinking that this case may warrant an undertaking because of the apparent lack of control of release of documents and the slow progress following the 2013 audit on refresher training. Tom, Laura what is your opinion?

I would recommend an informal resolution to this case because:

1. Although the documents are still not secure, a follow-up meeting (4 April 2016) of senior LBE figures from Families and Children and others reviewed the case from a safeguarding risk stance and considered that the risk should now be rated as low. FOIA s.44 - Prohibition on disclosure [redacted] There is no evidence, to date, of there being any unauthorised processing of the lost data.

2. LBE are reviewing and updating their Paper Records Secure Handling and Transit Policy to ensure it reflects social work practice and requirements.

3. Each area office will be supplied with lockable cases for use when transporting documents out of the office.

4. LBE are considering providing social workers with access to mobile working devices when attending court similar to that provided to the court team.

5. Roles and responsibilities for printing and transporting documents required as part of the court bundle should be clarified and confirmed with Legal. The outcome should be cascaded to social work teams.

I would recommend that LBE prepare and forward to the ICO an improvement plan covering:

1. A specific target date for 100% completion of refresher training. (currently standing at 68%).
   This was also an outstanding item from the ICO audit of 13-15 May 2013 (item a13) and action plan 20140120 (item 4.2 second bullet point). The audit follow-up in 2014 suggested that this was one of the outstanding actions that should be prioritised for completion.

2. Specific start and completion dates for team-based refresher data protection training to include locums.

And, from the LBE Management Investigation Report Recommendations:

3. Target date for completion of review and update of the Paper Records Secure Handling and Transit Policy.

4. Target date for making lockable cases available in each area office.

5. Target date for completion of review of making home working electronic devices available to social workers.

6. Target date for completion of review with Legal with regard to roles and responsibilities for printing and transporting documents required as part of court bundles.

Also to recommend that:

The manager's role in implementing clause 2.3 of the Paper Records Secure Handling and Transit Policy and enforcing clause 2.1.3 and 2.2 is either reviewed or reinforced and that training gaps are identified and corrected.

Team Manager Recommendations

Name: Laura Middleton
Date: 25 August 2016

Comments:
I agree that an undertaking would seem appropriate in this case. This is because, whilst we have not had any cases with this council in the last two years, they have previously been subject to enforcement action by way of a CMP. Further, the council was audited in 2013 and has still not complied with the recommendations regarding mandatory refresher training. I am of the view that an informal closure is unlikely to achieve compliance, and requiring an improvement plan and then an undertaking if progress is insufficient just prolongs the issue.

You just need to turn the recommendations you have made on their head to come up with specific steps the DC needs to take. For example, regarding locums we would need to say something like "implement a mechanism to allow monitoring of

DPA training undertaken by locums, and ensure all locums have received this training within six months". I would suggest six months is an appropriate timeframe for each of the steps. The council can come back and let us know if any of these timescales are not achievable.

Tom can advise you on the drafting on the undertaking and then it needs to come to me for review.

Pre – Meet

Individuals Present:
Date:

Comments and recommendation:

VERSION CONTROL

Author	Nicholas Martin
Department	Enforcement
First Draft	Sept 2012
Final version	Jan 2013 V1.3
Amendments	V.1 amended to remove the middle recommendation section. V.1.2 Intelligence Log reference added to ICO Involvement with DC section. V.1.3 Good Practice reference added to ICO Involvement with DC section and minor amendments to policies and training questions.

Hi [redacted]

If you have a query like this, could you put it on to the IP itself, perhaps in a different colour or highlighted by way of a comments box?

I use the provide advice process to try and reduce the number of emails in my inbox and I won't necessarily remember to marry emails about cases with the cases themselves!

I'm emailed this query to the case as a reminder to myself.

Thanks

Laura

From: [redacted]
Sent: 21 March 2016 08:59
To: Laura Middleton
Subject: COM0617270 - London Borough of Ealing - IP Forwarded for Review - Query

Good morning Laura

Hope you had a pleasant weekend.

I have transferred COM0617270 London Borough of Ealing to your queue for review of IP.

With regard to the effects of sensitive personal information being revealed to other parties: [redacted]

[redacted]

London Borough of Ealing

23 March 2016

Case reference number: **COM0617270**

Dear [redacted]

I am writing to confirm receipt of your email of 18 February 2016 reporting the loss of personal data, as defined by the Data Protection Act 1998 (DPA).

I am the case officer in charge of the investigation.

At this stage we are still investigating the circumstances you have reported to us, and we have not yet formed a view on what action, if any, we will take. However it is possible that, once we have considered all the relevant evidence, we will exercise our powers as set out in the attached leaflet. Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

The requirements of the Data Protection Act

I am investigating a potential breach of the seventh data protection principle. As you may be aware, the seventh principle requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

From the information I have at present, it appears that the data concerned may constitute sensitive personal data within the meaning of the DPA. [redacted]

Further information

In order that I may assess what further action may be necessary, I would be most grateful if you would provide the following information:

NB References made below (e.g. 4(f)) relate to responses contained in the council's original breach notification unless stated otherwise.

1. Have the documents been recovered to date? If so, please state when. If not, please state what, if anything, the council is doing to recover the documents.

2. Please provide a redacted copy of the type of data compromised in this incident and a sample of the most sensitive information.

3. [redacted]

4. Please provide a copy of any internal security incident report produced in connection with this incident.

5. Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed / processed? If so, please provide details.

6. Were the documents lost in this incident the only copies available? If so, please detail what effect, if any, the loss had on the care proceedings.

7. FOIA s.44 - Prohibition on disclosure [redacted]

8. Was it necessary to transport this amount of data for the purposes of this court attendance? If so, was it necessary that all data transported be in paper form?

9. Please explain why the data was transported in an envelope rather than in a secure case/bag or similar. Does the council require employees to use a secure case/bag when transporting personal data outside of council premises? Does the council provide such bags to employees? If so, please provide details of how employees are made aware of this. (This may be covered, in part, by 10. Below).

10. Please provide full copies of the current Data Protection Policy and Paper Records Policy detailed in 2(f). Also any other written policy or procedure relevant to the specific circumstances of this breach and describe any relevant policy or procedure which is not documented.

11. From the audit carried out by the ICO 13-15 May 2013 mention is made in the audit report (item a27) of a 'Paper Records Secure Handling and Transit Policy'. If this is different to the policy referred to in 9. above and is extant, please forward a full copy of this procedure.

12. Please describe how you bring these policies to your employees' attention.

13. Does the council have any procedures in place to track which paper records have been removed from the office, by whom and for what purpose? If so, please describe or forward relevant sections.

14. Do you consider the employee involved to have breached any of the organisation's policies or procedures? If so which policies or procedures? Please inform us of the disciplinary action taken, if any, in relation to the employee involved in this incident.

15. I note from the ICO audit issued in June 2013 that the council agreed to develop mandatory data protection refresher training (recommendation a13). Please confirm whether the council now requires employees to complete mandatory data protection refresher training. If refresher training is required how frequently does this training occur? Please provide details as to the measures you had in place to ensure that all staff attend any mandatory refresher training. Also, please provide up-to-date statistics regarding completion of training.

16. Can you confirm that the employee involved in this incident received the above mentioned data protection training? If so, when did they last receive this training prior to this incident?

17. Similarly, a9 from the audit report: "LBE are currently trialling 'MetaCompliance' policy management software" and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

18. In the light of the response given in 4(c), has the proposed action to minimise the possibility of a repeat of such an incident been completed? How was this action carried out and by what means was this verified/recorded?

19. Has the organisation put in place any other containment or safeguarding measures other than those detailed in the breach notification

20. As a result of this incident, did the organisation consider whether any other sensitive personal data held by your organisation may be exposed to similar vulnerabilities? If so, what steps were taken to address this?

21. Please forward a copy of the notification letter FOIA s.44 - Prohibition on disclosure detailed in your response to 3(c).

22. Since the notification, has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

Since the notification, has there been any media coverage of the incident? If so, please provide details.
If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Please provide the information requested by [DATE]. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

Thank you for reporting this incident.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fall und
Case Officer
Information Commissioner's Office
01625 545300

Good morning [redacted]

Please disregard my previous e-mail as I had not included a request for completion date.

My apologies for any inconvenience caused.

Best regards

[redacted]
Case Officer

AMENDED MESSAGE:

London Borough of Ealing

23 March 2016

Case reference number: **COM0617270**

Dear [redacted]

I am writing to confirm receipt of your email of 18 February 2016 reporting the loss of personal data, as defined by the Data Protection Act 1998 (DPA).

I am the case officer in charge of the investigation.

At this stage we are still investigating the circumstances you have reported to us, and we have not yet formed a view on what action, if any, we will take. However it is possible that, once we have considered all the relevant evidence, we will exercise our powers as set out in the attached leaflet. Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

The requirements of the Data Protection Act

I am investigating a potential breach of the seventh data protection principle. As you may be aware, the seventh principle requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

From the information I have at present, it appears that the data concerned may constitute sensitive personal data within the meaning of the DPA. [redacted]

Further information

In order that I may assess what further action may be necessary, I would be most grateful if you would provide the following information:

NB References made below (e.g. 4(f)) relate to responses contained in the council's original

breach notification unless stated otherwise.

1. Have the documents been recovered to date? If so, please state when. If not, please state what, if anything, the council is doing to recover the documents.

2. Please provide a redacted copy of the type of data compromised in this incident and a sample of the most sensitive information.

3. FOIA s.44 - Prohibition on disclosure [redacted]

4. Please provide a copy of any internal security incident report produced in connection with this incident.

5. Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed / processed? If so, please provide details.

6. Were the documents lost in this incident the only copies available? If so, please detail what effect, if any, the loss had on the care proceedings.

7. FOIA s.44 - Prohibition on disclosure [redacted]

8. Was it necessary to transport this amount of data for the purposes of this court attendance? If so, was it necessary that all data transported be in paper form?

9. Please explain why the data was transported in an envelope rather than in a secure case/bag or similar. Does the council require employees to use a secure case/bag when transporting personal data outside of council premises? Does the council provide such bags to employees? If so, please provide details of how employees are made aware of this. (This may be covered, in part, by 10. Below).

10. Please provide full copies of the current Data Protection Policy and Paper Records Policy detailed in 2(f). Also any other written policy or procedure relevant to the specific circumstances of this breach and describe any relevant policy or procedure which is not documented.

11. From the audit carried out by the ICO 13-15 May 2013 mention is made in the audit report (item a27) of a 'Paper Records Secure Handling and Transit Policy'. If this is different to the policy referred to in 9. above and is extant, please forward a full copy of this procedure.

12. Please describe how you bring these policies to your employees' attention.

13. Does the council have any procedures in place to track which paper records have been removed from the office, by whom and for what purpose? If so, please describe or forward relevant sections.

14. Do you consider the employee involved to have breached any of the organisation's policies or procedures? If so which policies or procedures? Please

inform us of the disciplinary action taken, if any, in relation to the employee involved in this incident.

15. I note from the ICO audit issued in June 2013 that the council agreed to develop mandatory data protection refresher training (recommendation a13). Please confirm whether the council now requires employees to complete mandatory data protection refresher training. If refresher training is required how frequently does this training occur? Please provide details as to the measures you had in place to ensure that all staff attend any mandatory refresher training. Also, please provide up-to-date statistics regarding completion of training.

16. Can you confirm that the employee involved in this incident received the above mentioned data protection training? If so, when did they last receive this training prior to this incident?

17. Similarly, a9 from the audit report: "LBE are currently trialling 'MetaCompliance' policy management software" and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

18. In the light of the response given in 4(c), has the proposed action to minimise the possibility of a repeat of such an incident been completed? How was this action carried out and by what means was this verified/recorded?

19. Has the organisation put in place any other containment or safeguarding measures other than those detailed in the breach notification

20. As a result of this incident, did the organisation consider whether any other sensitive personal data held by your organisation may be exposed to similar vulnerabilities? If so, what steps were taken to address this?

21. Please forward a copy of the notification letter FOIA s.44 - Prohibition on disclosure detailed in your response to 3(c).

22. Since the notification, has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

23. Since the notification, has there been any media coverage of the incident? If so, please provide details.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Allowing for bank holidays and as FOIA s.40(2) - Personal data that doesn't fall under s.40(1) please provide the information requested by 3 May 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

Thank you for reporting this incident.

I look forward to hearing from you.

Yours sincerely

[redacted]
Case Officer
Information Commissioner's Office
01625 545300

We are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the Data Protection Act 1998 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk). Please say whether you consider any of the information you send us is confidential. You should also say why. We will only withhold information where there is good reason to do so.

Dear [redacted]

I write further to your email received 24th March 2016.

As per your email please find further information that you have requested in respect of this data breach notification.

1. Have the documents been recovered to date? If so, please state when. If not, please state what, if anything, the council is doing to recover the documents.

No, the documents have not been recovered despite the several avenues mentioned in the notification to recover them. The Court concerned is aware the documents have been lost and we have been advised that they will contact us in the event they are handed in to the Court Office. We do not consider there to any further avenue to explore but are willing to do so if one is notified.

2. Please provide a redacted copy of the type of data compromised in this incident and a sample of the most sensitive information.

[redacted]

They have written to the Court to request the approval of the Judge to the release of these documents and they will follow once the approval of the Court has been obtained. If we are not given approval to release these documents I will advise you accordingly.

3. [redacted]

4. Please provide a copy of any internal security incident report produced in connection with this incident.

Please find attached.

5. Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed / processed? If so, please provide details.

No, we do not have any evidence to date that the personal data has been inappropriately accessed or processed.

6. Were the documents lost in this incident the only copies available? If so, please detail what effect, if any, the loss had on the care proceedings.

[redacted] A handwritten document had to be prepared at the last minute because the Local Authority were seeking to obtain [redacted]

However, these were not used in evidence and therefore had no effect on the care proceedings which are part heard.

7. FOIA s.44 - Prohibition on disclosure [redacted]

We have no evidence to suggest that there will be a safeguarding risk. Since the immediate notification of the affected subjects with named contact personnel for them and their counsel to contact in the event of experiencing any threat and the passage of time. At a follow up meeting on 4th April 2016, which was attended by the Interim Director of Children and Families, Assistant Director of Children and Families, the council's Caldicott Guardian, representatives from Data Protection and the Legal section it was considered that the risk should be now rated as 'low'.

8. Was it necessary to transport this amount of data for the purposes of this court attendance? If so, was it necessary that all data transported be in paper form?

It was considered necessary to have the information that was taken to court. FOIA s.44 - Prohibition on disclosure [redacted]

The WIFI capability at the court is known and accepted to be problematic and has caused difficulties in the past. The Court acknowledges this. In the circumstances, it was felt that taking physical papers would ensure all the information necessary for the hearing was available to the Social Worker without any issues of connectivity.

9. Please explain why the data was transported in an envelope rather than in a secure case/bag or similar. Does the council require employees to use a secure case/bag when transporting personal data outside of council premises? Does the council provide such bags to employees? If so, please provide details of how employees are made aware of this. (This may be covered, in part, by 10. Below).

The corporate Paper Records Handling Policy gives clear guidance in respect of handling data outside of the office. It advises that staff should not carry paper records/hard-copy materials 'loosely' as this increases the risk of dropping or losing them, or that they come loose from the rest of the file.
Lockable bags had previously been provided by the service area but it is clear on this occasion that the policy was not adhered to.
The Paper Records Handling Policy advises that :-

Managers must have proper approval procedures and controls in place within their teams to ensure that personal data or other confidential data contained in paper records/hard-copy material is only taken off-site:-

I. when it is necessary, rather than merely convenient, to achieve a specific task;

II. for the minimum time necessary to achieve that task, and

III. in circumstances where removal is limited to the minimum amount of information necessary to achieve that task.

How managers implement the necessary arrangements and monitor compliance with this policy is for them to decide, taking account of the particular requirements of the services that their teams deliver. However, in the event that a team, for which they are responsible, suffers a loss of personal or other confidential data contained in paper records/hard-copy material taken off-site, they will need to be able to satisfactorily demonstrate that they had ensured (i) proper approval procedures and controls were in place and (ii) the procedures and controls were adhered to through adequate and appropriate checks and considerations prior to the removal in question.

10. Please provide full copies of the current Data Protection Policy and Paper Records Policy detailed in 2(f). Also any other written policy or procedure relevant to the specific circumstances of this breach and describe any relevant policy or procedure which is not documented.

Please find attached.

11. From the audit carried out by the ICO 13-15 May 2013 mention is made in the audit report (item a27) of a ﷺPaper Records Secure Handling and Transit Policy﷽. If this is different to the policy referred to in 9. above and is extant, please forward a full copy of this procedure.

This is the same as the policy provided in Point 10

12. Please describe how you bring these policies to your employees﷽ attention.

All new staff receive data protection training as part of their induction. All staff within the Children﷽s Directorate are required to complete the online Data Protection training module. The data protection team provides training at the induction day for new starters within Children﷽s services. Before staff are allowed to use the case management system, they are required to attend a training course which includes data protection awareness.

Council policies are communicated to all new staff during their induction and are accessible on the intranet. Employee contracts also include the policies to be confirmed as read and understood with their line manager. In addition, all new starters must complete the online data protection module. The data protection team provides focused training to the organisation throughout the year.

13. Does the council have any procedures in place to track which paper records have been removed from the office, by whom and for what purpose? If so, please describe or forward relevant sections.

The corporate Paper Records Secure Handling and Transit Policy states:

1.1 Principles to be adopted:

1. There is a general presumption against taking off-site personal or other confidential data contained within paper records/hard copy material.
2. Personal or other confidential data contained within paper records/hard copy material should only be taken off-site when it is a necessity and not a convenience.
3. Line management approval must be obtained before personal or other confidential data contained within paper records/hard copy material is taken off-site. This approval request must provide details of the personal or other confidential data proposed to be taken off-site and the necessity for doing so and the relevant times (see 2.2).
4. Where personal or other confidential data contained within paper records/ hard copy material is taken off-site it should be kept to a minimum both in terms of content and duration.
5. Whilst off-site and temporarily in the home of an employee (or other person covered by the policy), paper records/hard copy material containing personal or other confidential data, that is not being actively worked upon, must be kept secure and separate from any valuable items such as laptops.
6. Where personal or other confidential data contained within paper records/hard copy material is taken off-site and is in transit from one location to another, it should be transported in a way that mitigates against the risks of theft or loss.

14. Do you consider the employee involved to have breached any of the organisation﷽s policies or procedures? If so which policies or procedures? Please inform us of the disciplinary action taken, if any, in relation to the employee involved in this incident.

We do consider that the employee breached the requirements of the Paper Handling Policy as described above and also the Data Protection Policy which states the following :-

Employee & Member Responsibility

All Council personnel are personally responsible and accountable for ensuring compliance with the principles of the Act and that their use and handling of personal data is in accordance with the purpose(s) the Council have notified to the Information Commissioner. Adherence to the Act forms part of Council's Code of Conduct and contract of employment.
Please be advised that the employee has subsequently resigned from her position in the organisation.

15. I note from the ICO audit issued in June 2013 that the council agreed to develop mandatory data protection refresher training (recommendation a13). Please confirm whether the council now requires employees to complete mandatory data protection refresher training. If refresher training is required how frequently does this training occur? Please provide details as to the measures you had in place to ensure that all staff attend any mandatory refresher training. Also, please provide up-to-date statistics regarding completion of training.

All staff within Children's services have been asked to complete the online data protection training. This will be required to be completed yearly. The Corporate Data Protection Policy has been sent to all staff via Metacompliance and will be sent out annually to remind staff of their obligations.

16. Can you confirm that the employee involved in this incident received the above mentioned data protection training? If so, when did they last receive this training prior to this incident?

I am advised that the employee undertook data protection training in 2014 and would have been requested to undertake the e learning data protection training.

17. Similarly, a9 from the audit report: "LBE are currently trialling "MetaCompliance" policy management software" and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

Metacompliance has been successfully implemented within the organisation. A programme of disseminating policies is in place. The Data Protection Policy has been sent to all staff. I will forward separate to this email the statistics regarding training.

18. In the light of the response given in 4(c), has the proposed action to minimise the possibility of a repeat of such an incident been completed? How was this action carried out and by what means was this verified/recorded?

The management investigation that took place identified gaps in the procedure of taking paper records out of the office. Recommendations have been made as part of a management investigation and include:

- Advice and guidance contained in the "Paper Records Secure Handling and Transit Policy" will be updated and reviewed to ensure that it reflects social work practice and requirements. Details of the requirements should be widely circulated within social care and a link created in tri-x. Workers have been reminded of the principles of secure paper handling in the interim.
- Specific guidance to be given to workers regarding the storage of confidential information at home. It should be made clear that, unless agreed storage is available, this is an exceptional circumstance. Documentation should be destroyed using council confidential waste facilities as soon as possible. A formal process for the provision of lockable home storage should be devised.
- Each area office should have lockable cases available for workers who are required to transport papers out of the office. These should be kept securely and usage appropriately controlled.
- Consideration to be given to providing social workers from localities teams with access to mobile working devices when attending court, in a similar way to that provided to the court team.
- Roles and responsibilities for printing and transporting documents required as part of the court bundle should be clarified and confirmed with Legal. The outcome should be cascaded to social work teams.
- All Social Care staff that has not yet completed e learning modules: Data Protection & Information Sharing and Confidentiality (Social Care), are required to do so as soon as possible.

19. Has the organisation put in place any other containment or safeguarding measures other than those detailed in the breach notification

The organisation considers that the containment and safeguarding measures are sufficient in the circumstances and no further containment and safeguarding measures have been put in place.

20. As a result of this incident, did the organisation consider whether any other sensitive personal data held by your organisation may be exposed to similar vulnerabilities? If so, what steps were taken to address this?

The Paper Records Handling policy is being reviewed by all directorates with a view to identifying any possible vulnerability. Consideration is being given to adopting the Legal Team's procedure for taking information to court in the social care departments. This involves transporting documents in accordance with the Paper records Secure Handling and Transit Policy. The Legal Team are currently in advanced stages of investigating electronic bundling which provides for a secure cloud based system to share information with the Court and other parties.

21. Please forward a copy of the notification letter FOIA s.44 - Prohibition on disclosure detailed in your response to 3(c).

Please find attached.

22. Since the notification, has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

No, we have not received a formal complaint from any individual affected by this breach.

23. Since the notification, has there been any media coverage of the incident? If so, please provide details.

No, there has not been any media coverage of this incident.

24. If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

As responded to question 18., the corporate Paper Handling and Transit Policy is being reviewed and updated to reflect the specific needs of social care services.

Once agreed, the policy will be actively communicated as part of data protection training at induction days and become standing agenda items for team meetings.

The already mandatory online data protection training has been asked to be completed as a refresher by social care staff and will be monitored to ensure compliance. All staff in the Social Care and Education Legal team has undertaken an e-learning module in relation to data protection.

Finally, I hope this clarifies the situation but if you have any further queries please do not hesitate to contact me.

Yours sincerely

FOIA s.44 - Prohibition on di
Corporate Information Governance Manager
020 8825 5512

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 24 March 2016 11:25
To: FOIA s.44 - Prohibition on di
Subject: AMENDMENT:ICO Ref.: COM0617270 Breach Notification FOIA s.44 - Prohibitio - Further Information Required[Ref. COM0617270]

Good morning [redacted]

Please disregard my previous e-mail as I had not included a request for completion date.

My apologies for any inconvenience caused.

Best regards

[redacted]
Case Officer

AMENDED MESSAGE:

London Borough of Ealing

23 March 2016

Case reference number: **COM0617270**

Dear [redacted]

I am writing to confirm receipt of your email of [redacted] reporting the loss of personal data, as defined by the Data Protection Act 1998 (DPA).

I am the case officer in charge of the investigation.

At this stage we are still investigating the circumstances you have reported to us, and we have not yet formed a view on what action, if any, we will take. However it is possible that, once we have considered all the relevant evidence, we will exercise our powers as set out in the attached leaflet. Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

The requirements of the Data Protection Act

I am investigating a potential breach of the seventh data protection principle. As you may be aware, the seventh principle requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

From the information I have at present, it appears that the data concerned may constitute sensitive personal data within the meaning of the DPA. [redacted]

Further information

In order that I may assess what further action may be necessary, I would be most grateful if you would provide the following information:

NB References made below (e.g. 4(f)) relate to responses contained in the council's original breach notification unless stated otherwise.

1. Have the documents been recovered to date? If so, please state when. If not, please state what, if anything, the council is doing to recover the documents.

2. Please provide a redacted copy of the type of data compromised in this incident and a sample of the most sensitive information.

3. FOIA s.44 - Prohibition on disclosure [redacted]

4. Please provide a copy of any internal security incident report produced in connection with this incident.

5. Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed / processed? If so, please provide details.

6. Were the documents lost in this incident the only copies available? If so, please detail what effect, if any, the loss had on the care proceedings.

7. FOIA s.44 - Prohibition on disclosure [redacted]

8. Was it necessary to transport this amount of data for the purposes of this court attendance? If so, was it necessary that all data transported be in paper form?

9. Please explain why the data was transported in an envelope rather than in a secure case/bag or similar. Does the council require employees to use a secure case/bag when transporting personal data outside of council premises? Does the council provide such bags to employees? If so, please provide details of how employees are made aware of this. (This may be covered, in part, by 10. Below).

10. Please provide full copies of the current Data Protection Policy and Paper Records Policy detailed in 2(f). Also any other written policy or procedure relevant to the specific circumstances of this breach and describe any relevant policy or procedure which is not documented.

11. From the audit carried out by the ICO 13-15 May 2013 mention is made in the audit report (item a27) of a "Paper Records Secure Handling and Transit Policy". If this is different to the policy referred to in 9. above and is extant, please forward a full copy of this procedure.

12. Please describe how you bring these policies to your employees' attention.

13. Does the council have any procedures in place to track which paper records have been removed from the office, by whom and for what purpose? If so, please describe or forward relevant sections.

14. Do you consider the employee involved to have breached any of the organisation's policies or procedures? If so which policies or procedures? Please inform us of the disciplinary action taken, if any, in relation to the employee involved in this incident.

15. I note from the ICO audit issued in June 2013 that the council agreed to develop mandatory data protection refresher training (recommendation a13). Please confirm whether the council now requires employees to complete mandatory data protection refresher training. If refresher training is required how frequently does this training occur? Please provide details as to the measures you had in place to ensure that all staff attend any mandatory refresher training. Also, please provide up-to-date statistics regarding completion of training.

16. Can you confirm that the employee involved in this incident received the above mentioned data protection training? If so, when did they last receive this training prior to this incident?

17. Similarly, a9 from the audit report: 'LBE are currently trialling 'MetaCompliance' policy management software' and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

18. In the light of the response given in 4(c), has the proposed action to minimise the possibility of a repeat of such an incident been completed? How was this action carried out and by what means was this verified/recorded?

19. Has the organisation put in place any other containment or safeguarding measures other than those detailed in the breach notification

20. As a result of this incident, did the organisation consider whether any other sensitive personal data held by your organisation may be exposed to similar vulnerabilities? If so, what steps were taken to address this?

21. Please forward a copy of the notification letter FOIA s.44 - Prohibition on disclosure detailed in your response to 3(c).

22. Since the notification, has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

23. Since the notification, has there been any media coverage of the incident? If so, please provide details.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Allowing for bank holidays and as FOIA s.40(2) - Personal data that doesn't fall under s.40(1) please provide the information requested by 3 May 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

Thank you for reporting this incident.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fa
Case Officer
Information Commissioner's Office
01625 545300

We are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the Data Protection Act 1998 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk). Please say whether you consider any of the information you send us is confidential. You should also say why. We will only withhold information where there is good reason to do so.

---

attachment is virus free or has not been intercepted and amended. You should perform your own virus checks.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Tel: 0303 123 1113 Fax: 01625 524 510 Web: www.ico.org.uk

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 24 March 2016 11:25
To: [redacted]
Subject: AMENDMENT:ICO Ref.: COM0617270 Breach Notification [redacted] - Further Information Required[Ref. COM0617270]

Good morning [redacted]

Please disregard my previous e-mail as I had not included a request for completion date.

My apologies for any inconvenience caused.

Best regards

[redacted]
Case Officer

AMENDED MESSAGE:

London Borough of Ealing

23 March 2016

Case reference number: **COM0617270**

Dear [redacted]

I am writing to confirm receipt of your email of [redacted] reporting the loss of personal data, as defined by the Data Protection Act 1998 (DPA).

I am the case officer in charge of the investigation.

At this stage we are still investigating the circumstances you have reported to us, and we have not yet formed a view on what action, if any, we will take. However it is possible that, once we have considered all the relevant evidence, we will exercise our powers as set out in the attached leaflet. Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore

appreciated.

The requirements of the Data Protection Act

I am investigating a potential breach of the seventh data protection principle. As you may be aware, the seventh principle requires appropriate technical and organisational measures to be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

From the information I have at present, it appears that the data concerned may constitute sensitive personal data within the meaning of the DPA. This is because the data appears to include information about Looked After Children who may be at risk.

Further information

In order that I may assess what further action may be necessary, I would be most grateful if you would provide the following information:

NB References made below (e.g. 4(f)) relate to responses contained in the council's original breach notification unless stated otherwise.

1. Have the documents been recovered to date? If so, please state when. If not, please state what, if anything, the council is doing to recover the documents.
2. Please provide a redacted copy of the type of data compromised in this incident and a sample of the most sensitive information.
3. FOIA s.44 - Prohibition on disclosure [redacted]
4. Please provide a copy of any internal security incident report produced in connection with this incident.
5. Is there any evidence to date that the personal data involved in this incident has been inappropriately accessed / processed? If so, please provide details.
6. Were the documents lost in this incident the only copies available? If so, please detail what effect, if any, the loss had on the care proceedings.
7. FOIA s.44 - Prohibition on disclosure [redacted]
8. Was it necessary to transport this amount of data for the purposes of this court attendance? If so, was it necessary that all data transported be in paper form?

9. Please explain why the data was transported in an envelope rather than in a secure case/bag or similar. Does the council require employees to use a secure case/bag when transporting personal data outside of council premises? Does the council provide such bags to employees? If so, please provide details of how employees are made aware of this. (This may be covered, in part, by 10. Below).

10. Please provide full copies of the current Data Protection Policy and Paper Records Policy detailed in 2(f). Also any other written policy or procedure relevant to the specific circumstances of this breach and describe any relevant policy or procedure which is not documented.

11. From the audit carried out by the ICO 13-15 May 2013 mention is made in the audit report (item a27) of a "Paper Records Secure Handling and Transit Policy". If this is different to the policy referred to in 9. above and is extant, please forward a full copy of this procedure.

12. Please describe how you bring these policies to your employees' attention.

13. Does the council have any procedures in place to track which paper records have been removed from the office, by whom and for what purpose? If so, please describe or forward relevant sections.

14. Do you consider the employee involved to have breached any of the organisation's policies or procedures? If so which policies or procedures? Please inform us of the disciplinary action taken, if any, in relation to the employee involved in this incident.

15. I note from the ICO audit issued in June 2013 that the council agreed to develop mandatory data protection refresher training (recommendation a13). Please confirm whether the council now requires employees to complete mandatory data protection refresher training. If refresher training is required how frequently does this training occur? Please provide details as to the measures you had in place to ensure that all staff attend any mandatory refresher training. Also, please provide up-to-date statistics regarding completion of training.

16. Can you confirm that the employee involved in this incident received the above mentioned data protection training? If so, when did they last receive this training prior to this incident?

17. Similarly, a9 from the audit report: "LBE are currently trialling "MetaCompliance" policy management software" and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

18. In the light of the response given in 4(c), has the proposed action to minimise the possibility of a repeat of such an incident been completed? How was this action carried out and by what means was this verified/recorded?

19. Has the organisation put in place any other containment or safeguarding measures other than those detailed in the breach notification

20. As a result of this incident, did the organisation consider whether any other sensitive personal data held by your organisation may be exposed to similar vulnerabilities? If so, what steps were taken to address this?

21. Please forward a copy of the notification letter [redacted] detailed in your response to 3(c).

22. Since the notification, has the organisation received a formal complaint from any individual affected by this breach? If so, please provide details.

23. Since the notification, has there been any media coverage of the incident? If so, please provide details.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Allowing for bank holidays and as [redacted] please provide the information requested by 3 May 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

Thank you for reporting this incident.

I look forward to hearing from you.

Yours sincerely

[redacted]
Case Officer
Information Commissioner's Office
01625 545300

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Tel: 0303 123 1113 Fax: 01625 524 510 Web: www.ico.org.uk

Ealing Council

Corporate ICT & Data Management

Data Protection Policy

Classification:	Unclassified
Date Created:	January 2012
Date Reviewed	January 2016
Version:	2.0
Author:	FOIA s.44 - Prohibition on disclosure
Owner:	FOIA s.44 - Prohibition on disclosure Corporate Information Governance Manager

Version Control

Date	Change Description	Author	Version
January 2016	Revised and updated	[redacted]	2.0

Reviewers			
Name	**Title / Role**	**Date of Issue**	**Version**
[redacted]	Head of Strategic ICT & Data Management	January 2016	
[redacted]	Corporate ICT & Data Security Manager	January 2016	
[redacted]	Infrastructure & Technical assurance Manager	January 2016	

Policy Approved By			
Title/Role	**Name**	**Date approved**	**Version**
Interim Director of Business Services Group	[redacted]	January 2016	2.0
Director of Legal and Democratic Services	[redacted]	[redacted] 2016	2.0

Policy Distribution after approval			
Title/Role	**Name**	**Date approved**	**Version**
All staff			

Introduction

The London Borough of Ealing is committed to ensuring the privacy of the individual is respected and that all personal data that is processed by the organisation is dealt with in accordance with the Principles of the Data Protection Act 1998 (the “Act”).

The Act is designed to safeguard personal data and allow organisations such as the Council to collect and process this data for legitimate purposes.

All Council employees need to ensure that other people’s information is protected and kept safe at all times. If personal information is taken from one location to another it must be done so as a necessity and not as a convenience and it must be done so in the safest possible way. We must ensure equipment is fully password protected and encrypted, and kept secure at all times. Files, diaries, notepads or computer equipment must never be left unattended.

Any queries about Data Protection employee obligations or the rights of individuals and members of the public in relation to information about themselves should be directed to the Corporate Data Protection team.

2.0 Purpose

The Council needs to collect and use personal data about individuals, residents, customers, employees (present, past and prospective), suppliers, contractors and other businesses, in order to meet its statutory obligations and provide its services. No matter how personal data is collected or held, either manually or electronically, it must be handled and processed properly to ensure that the Council meets its legal obligation to comply with the principles of the Data Protection Act 1998 (the Act).

The Act places obligations on organisations, such as the Council, which process [1] personal data [2], and protects the rights and freedoms of the individuals who are subjects of that data.

The purpose of this policy is to:

- explain the Council's commitment to the lawful and fair treatment of personal data and its intent to comply with the principles of the Act.
- ensure that all personnel, elected members [3] and partners [4] are made aware of their responsibilities under the Act; and
- ensure that all employees, elected members and partners are aware of the rights of data subjects[5] and ensure that those rights are protected.

3.0 Scope

This policy applies to all personnel whether employed directly by the Council or by a "partner", members and any other individual who has access to personal data collected, owned and/or used by the Council.

---

1 Processing in relation to data includes obtaining, recording, holding, using or disclosing,
2 Personal data is data that relates to an identifiable living individual.
3 Elected members need to understand in what capacity they are acting under the provisions of the Act
4 A partner includes contractors, consultants, agency staff, service providers etc.
5 A data subject is an individual to whom the data relates.

4.0 The Council's Commitment

The Council, through the appropriate application of managerial and operational controls, will:

- only process personal data fairly and lawfully and in accordance with all required conditions
- specify the purpose(s) for which personal data is being used; (this is defined in the Council's Privacy Notice)
- only collect the personal data that is necessary to fulfil the operational needs of any service provided or to comply with legislative or organisational requirements;
- take steps to ensure the quality and integrity of personal data used;
- put in place the appropriate measures to ensure that personal data is only retained for as long as it is needed for the purpose(s) it was obtained for, or to meet legal requirements;
- ensure that the rights of every individual who provides the Council with personal data are respected;
- provide the appropriate technical and organisational security measures that will safeguard personal data against unauthorised or unlawful processing, accidental loss, destruction or damage;
- ensure that personal data is not transferred outside the European Economic Area without the appropriate safeguards.

In addition to the above the Council will endeavour, through the distribution of guidance material and training, to ensure that:

- all processing of personal data undertaken by the Council is notified to the Information Commissioner's Office;
- all employees managing and handling personal data are aware of and understand their responsibilities under the Act;
- every individual managing and handling personal data is appropriately trained to do so;
- every individual understands the purpose(s) for which they are processing personal data and also under what circumstances further processing may take place;
- every individual managing and handling personal data understands the rights of the data subject;
- there is a post with overall responsibility for the monitoring of data protection legislation and compliance within the Council;
- there is a representative within each department/service to provide a communications network to ensure compliance with the Act.

5.0. Employee & Member Responsibility

All Council personnel are personally responsible and accountable for ensuring compliance with the principles of the Act and that their use and handling of personal data is in accordance with the purpose(s) the Council have notified to the Information Commissioner. Adherence to the Act forms part of Council's Code of Conduct and contract of employment.

Any personnel or member who fails to carry out their duty in compliance with the Act will be subject to disciplinary action.

All managers must ensure that any additional or new purpose for which they are processing personal data is notified to the Corporate Information Governance Manager, who will amend the Council's notification as appropriate.

6.0 Individual Rights

The Act gives rights to individuals in respect of personal data processed about them by the Council. These rights apply to all individuals, whether they are employees, elected members or members of the public. The Data Protection Act 1998 confers the following rights on data subjects:

- the right of access to personal data;
- the right to prevent processing likely to cause damage or distress;
- the right to prevent processing for purposes of direct marketing;
- rights in relation to automatic decision-taking;
- the right to compensation for failure by the Council to comply with the requirements of the Act;
- the right, via the courts, to rectify block, erase, or destroy inaccurate data; and
- the right to request an assessment, by the Information Commissioner, that the processing of personal data is in compliance with the Act.

7.0 Right of access

Subject to a limited number of exemptions, an individual has the right to be supplied with a copy of their personal data. This is called the subject access right and is the right that individuals are most likely to make use of. Requests must be in writing and the Council has 40 days in which to comply with a valid request.

All personnel should be able to recognise a request when received and be aware of the procedure for handling such requests (see the Intranet). If an employee is instructed to prepare a file in accordance with Section 7 of the Act they should be suitably trained and respond within the statutory time period.

8.0 The Information Commissioner's Office

The data protection powers of the Information Commissioner's Office are to:

- Conduct assessment to check organisations are complying with the Act;
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specific information within a certain time period;
- Service enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specific steps in order to ensure they comply with the law;
- Prosecute those who commit criminal offences under the Act;
- Conduct audits to assess whether organisations processing or personal data follows good practice; and
- Report to Parliament on data protection issues of concern.
- Issue monetary penalties to organisations who fail to comply with the Act

Appeals from Notices are heard by the Information Tribunal, an independent body set up specifically to hear cases concerning enforcement notices or decision notices issued by the Information Commissioner.

9.0 Criminal Offences

The Act creates a number of criminal offences. Failure to comply with the requirements of the Act could result in personnel being held liable under the Act for their actions.

The Act also provides for separate personal liability of directors and other staff where their consent, connivance or neglect has been instrumental in an offence committed by the corporate body.

All personnel should be aware that if found guilty of committing an offence under the Act, they could be liable for a fine of up to £5,000 in a Magistrates court or an unlimited fine in a Crown court.

10.0 The Data Protection Principles

There are **eight** Data Protection principles that must be adhered to. The following is a summary:

1. Personal data shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary kept up-to-date;
5. Personal data shall not be kept for longer than is necessary;
6. Personal data shall be processed in accordance with the rights of the data subject;
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to personal data;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures adequate levels of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Policy review

This policy will be reviewed annually. It will be amended in response to changes in operational and legal requirements. Every effort will be made to ensure individual users are made aware of changes when they occur.

The most current version of the policy will always be available on the Intranet and on request from the HR Shared Service Centre.

If you have any queries or questions about this policy contact the Corporate Information Governance Manager.

Appendix 1

DEFINITIONS

Knowledge of these definitions is important to an understanding of this policy.

Personal data means data which relate to a living individual who can be identified –

a) from those data, or

Personal data means data which relate to a living individual who can be identified –

(a) from those data, or (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be processing.

Sensitive personal data means personal data consisting of information as to -

(a) the racial or ethnic origin of the data subject,

(b) political opinions,

(c) religious beliefs or other beliefs of a similar nature,

(d) whether an individual is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),

(e) physical or mental health or condition,

(f) sexual life,

(g) the commission or alleged commission by the individual of any offence, or

(h) any proceedings for any offence committed or alleged to have been committed by the individual the disposal of such proceedings or the sentence of any court in such proceedings.

Data subject – means an individual who is the subject of personal data.

Data controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Relevant Legislation

Computer Misuse Act 1990

This Act makes it an offence for an unauthorised person to access knowingly a program or data or for such a person to modify knowingly the contents of a computer. The Police and Justice Act 2006 have increased the penalties under this act.

Data Protection Act 1998 (DPA)

This Act regulates the processing of personal data by organisations employers.

Ealing Council

Paper Records Secure Handling and Transit Policy - Including Remote Printing

Classification:	
Date Created:	
Date Approved:	
Review Due:	
Ref:	V2 2012
Author:	[redacted]
Owner:	Corporate Information and Data Management

Version Control

Document Change Control			
Date	Change Description	**Release**	Version
28/02/2012	Draft Version 1 Feb 2012		V1
03/03/2012	Draft Version 3 March 2012		V2

Distribution – this document has been distributed to:			
Name	**Title / Role**	**Date of Issue**	**Version**
FOIA s.44 - Prohibition on disclosure	Legal	Feb 2012	V1
	Legal	Feb 2012	V1
	Director of Children and Families	Feb2012	V1
	Director of Adult Services	Feb 2012	V1
	Corporate ICT Security	Feb 2012	V1
	Corporate Data Protection	Feb 2012	V1
	Head of Strategic ICT	Feb 2012	V1
	Caldicott Guardian	Feb 2012	V1
	Corporate Data Protection	Feb 2012	V1

Policy Approved By			
Title/Role	**Name**	**Date approved**	**Version**

Contents

1 Introduction and scope

With home and mobile working on the increase we need to be more aware of the limited circumstances in which paper records/hard copy material containing personal or other confidential data may be taken out of, or accessed away from the office. This policy sets out the nature of those limited circumstances and details the security measures that we need to adopt when transporting or storing papers/hard copy material off-site, particularly when such records contain personal or confidential data.

These security methods must be robust enough for the type of information in the records. This involves considering in each case;

- the value, sensitivity and confidentiality of the information being taken off site;
- the risk of the information being lost or stolen**;**
- the damage or distress that could be caused to individuals if their personal or other confidential data were to be lost or stolen, and;
- the reputational and financial damage that could be caused to the Council or other agencies or organisations as a result of a breach.

This policy applies to the Council's employees, contractors, agency workers, consultants, interims, temporary staff or third parties when accessing or using personal or confidential information held by the Council or doing so whilst otherwise acting on behalf of the Council.

Whilst primarily aimed at ensure compliance with the Data Protection Act 1998 ("DPA"), the measure in this policy must equally be applied to the transit and storage of other types of confidential information.

2 Taking paper records/hard copy material off-site

All Council employees and others covered by the policy, with access to personal other confidential data, must always give serious consideration as to whether it is necessary to take paper records/hard copy material containing personal data or other confidential information off-site. The reasons for taking such paper records/hard copy material off-site must always be one of necessity and not convenience.

Taking paper records/hard copy material off-site should only happen when it is absolutely essential to do so and there is no alternative method for accessing or online via an encrypted device. Where papers records/hard copy material have to be taken off-site, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed and, where possible, data should be anonymised.

All employees and others covered by the policy, with access to personal or other confidential data, are individually responsible for ensuring the adequate protection of information in their possession and ensuring its safe return.

The principles below are to be adopted and adhered to, to minimise the theft, loss or unauthorised use of personal or other confidential data whilst in transit or off-site.

2.1 Principles to be adopted:

1. There is a general presumption against taking off-site personal or other confidential data contained within paper records/hard copy material.

2. Personal or other confidential data contained within paper records/hard copy material should only be taken off-site when it is a necessity and not a convenience.

3. Line management approval must be obtained before personal or other confidential data contained within paper records/hard copy material is taken off-site. This approval request must provide details of the personal or other confidential data proposed to be take off-site and the necessity for doing so and the relevant times (see 2.2).

4. Where personal or other confidential data contained within paper records/ hard copy material is taken off-site it should be kept to a minimum both in terms of content and duration.

5. Whilst off-site and temporarily in the home of an employee (or other person covered by the policy), paper records/hard copy material containing personal or other confidential data, that is not being actively worked upon, must be kept secure and separate from any valuable items such as laptops.

6. Where personal or other confidential data contained within paper records/hard copy material is taken off-site and is in transit from one location to another, it should be transported in a way that mitigates against the risks of theft or loss.

7. This means that, insofar as possible, all necessary steps should be taken to seek to ensure that the paper records/hard copy material and/is not mistaken for a laptop, other electrical device or valuable item by a thief and should be transported in a separate container to such items.

2.2 Approval of requests

Should an incident occur it is important that we know immediately what information has potentially been lost or stolen. This allows us to properly assess the risks and possible issues, involved and, where necessary, to notify any affected third parties including, where appropriate, the Information Commissioner's Office and other relevant agencies.

Before taking paper records/hard–copy material containing personal or other confidential data off-site you must have:

- Notified your manager of the paper records/hard-copy material containing personal or other confidential data you intend to take off-site, and obtained his or her consent to do so.

- Made a note of the paper records / hard-copy material containing personal or other confidential data you intend to remove. The log should be kept on-site for reference in the event of any or all such records being lost or stolen.

2.3 Managers Responsibilities

Managers must have proper approval procedures and controls in place within their teams to ensure that personal data or other confidential data contained in paper records/hard-copy material is only taken off-site:-

I. when it is necessary, rather than merely convenient, to achieve a specific task;
II. for the minimum time necessary to achieve that task, and
III. in circumstances where removal is limited to the minimum amount of information necessary to achieve that task.

How managers implement the necessary arrangements and monitor compliance with this policy is for them to decide, taking account of the particular requirements of the services that their teams deliver. However, in the event that a team, for which they are responsible, suffers a loss of personal or other confidential data contained in paper records/hard-copy material taken off-site, they will need to be able to satisfactorily demonstrate that they had ensured (i) proper approval procedures and controls were in place and (ii) the procedures and controls were adhered to through adequate and appropriate checks and considerations prior to the removal in question.

2.4 Best practice guidance

If you have determined that it is necessary to take paper records/hard-copy material off-site, there are many practical actions you can take to minimise the risk of data loss. For example;

- don't carry paper records/hard-copy materials 'loosely' as this increased the risk of dropping or losing them, or that they come loose from the rest of the file;
- don't carry paper records/hard-copy material in the same bag as electronic device (lap-top) or in any bag containing valuables, as these are often the primary target for thieves;
- ensure paper records/hard-copy material are not in transit for any longer than is necessary, and they are delivered to their destination at the earliest opportunity;
- don't leave bags or cases containing paper files in the car.

- when travelling on public transport keep you bag/case containing paper records/files/hard-copy material close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of theft or the misplacement of the item;

- ensure paper records/hard copy materials are not away from the office for longer than is necessary and return them as soon as possible.

3 Dispatching records as "as-and-when" staff and home workers

There will be occasions where paper records/hard-copy materials need to be sent off-site to another person who is either working from home or is working on an "as-and-when" basis.

3.1 Protocols to be adopted

Personal or other confidential data should normally be transferred by secure email, through a secure network connection or on a fully encrypted Council supplied USB Stick. Operating within the Council's environment, ie name@ealing.gov.uk to name@ealing.gov.uk is secure. Downloading into a non-council environment presents a significant risk to information being compromised.

The new ICT strategy will provide a Secure Global Desktop facility which will enable staff to access all their environments from home securely during 2012.

Paper records/hard-copy material should only be used if there is a necessity to do so and there is no alternative. In such cases you must:-

- Consider and adopt the protocols stated in 2.1
- Choose a method of delivery appropriate to the nature of the information in the records, ensure its security at all times.
- Make the recipients of the information aware of their, and the Council's responsibilities under the DPA.
- Ensure the recipients adopt adequate security measures for the protection of the data whilst in transit and storage.

4 Training and Information

All employees and others covered by this policy who have access to personal or other confidential data, must be made aware by their line manager or the existence of the policy via their team induction and other briefing processes. Managers must highlight to individuals their responsibility→→and the importance of data protection/security.

Appropriate training is to be provided to all those with access to personal or other confidential data.

Whilst some briefings may be run centrally, line managers and senior offers within Directorates must ensure that those with access to personal or other confidential data are appropriately trained in data protection/security.

If you do not feel that you have received adequate training or information, then you must raise this with your line manager.

5. Disciplinary action and criminal offences

Although the Council is responsible for complying with the DPA, **employees may face internal disciplinary action** if they cause the Council to be in breach of its obligations by failing to follow Council policies and procedures.

The DPA also creates a range of **criminal offences** for which employees may be found personally liable, including;

- Unlawfully obtaining, disclosing or procuring the disclosure of personal data
- Selling, or offering to sell, personal data which has been unlawfully obtained.

6. Reporting a data loss

All data losses and other security breaches, including breaches of this policy must be reported immediately the employees line manager, the service area manager and to the Corporate Data Protection Manager, in line with the Council's Incident Reporting Procedure.

The promptness of reporting is vital in ensuring quick containment of the breach and, where possible, recovery of personal/confidential information. Any delay in reporting is likely to have a detrimental effect on the breach management process.

7. Review

This policy will be reviewed on an annual basis.

8. Advice and Contact Information

Further Data Protection advice and associated polices can be located on the Information and Data Management Internet page.

Specific advice and guidance is also available from the Corporate Data Protection Team;

Tel: No: FOIA s.44 - Prohibition on disclosure

dataprotection@ealing.gov.uk

9. Off-Council Site Printing

Corporate ICT and Data Management acknowledge the restrictions a reduced print function causes for remote workers. To assist, restrictions have for the present time been removed. However, all individuals who are now able to print Ealing Council material remotely (from home) must personally take precautions to ensure that material which they print is printed in a secure environment. This policy applies to the Secure Handling and Transfer of personal or other confidential data contained within paper records/hard copy material which has been printed outside Council premises by individuals.

Printing of such material must only be when absolutely necessary, and should be on a limited basis. Safeguarding personal or other confidential data whilst at the private property of an employee/contractor/agency worker is the responsibility of the individual. Every effort must be made to ensure that the printed personal and confidential data is adequately secured within a locked cabinet or suitable alternative. The destruction of personal and sensitive material must be completed in accordance with Ealing Council's destruction process, which is set out in Ealing Council's Corporate Retention and Disposal Guidelines. Failure to take appropriate security measures to protect services users personal and sensitive information may result in disciplinary action, including dismissal, being taken against Council Employees, and may result, in the termination of arrangements with contractors or agency workers.

Ealing Council

www.ealing.gov.uk

PRIVATE AND CONFIDENTIAL

Ealing Council
Ealing Council
Perceval House 3:SE
14-16 Uxbridge Road
London W5 2HL
Tel: (020) 8825 5000

Your Ref	My Ref	Date	Please ask for	Direct line/ext.
		15/01/2025	FOIA s.44 - Prohibition on disclosure	

Dear ,

FOIA s.44 - Prohibition on disclosure

I am writing to advise you that information about this matter held by Ealing Council was unfortunately compromised recently.

This incident occurred because the Social Worker inadvertently forgot to take the documents with her on leaving the West London Family Court on Thursday, 4th February. Please be advised that the Council has tried to do what we can to recover the documents that have been lost. The steps taken to recover the documents have included searches of the car park and enquiries of the Court and neighbouring buildings and enquiries of the police. At present, these documents have not been recovered.

FOIA s.44 - Prohibition on disclosure

Ealing Council works to help and support adults, children and young people every day and we take these duties extremely seriously. I am very sorry that we have on this occasion, failed to meet our own high standards and I would like to offer you my sincere apologies for this matter.

I do understand this will be of concern to you and I appreciate that you may wish to discuss this further. The team manager, FOIA s.44 - Prohibition on disclosure, within our Social Care department

is available to answer any queries that you may have in respect of the information that was compromised. If you wish to speak with her, her direct line is FOIA s.44 - Prohibition on disclosure

Finally, once again please accept my apologies for this matter and if I can be of any assistance to you please do not hesitate to contact me.

Yours sincerely

FOIA s.44 - Prohibition on disclosure

Corporate Information Governance Manager

DATA SECURITY BREACH MANAGEMENT GUIDELINES

CONFIDENTIAL

MANAGEMENT INVESTIGATION REPORT INTO the [redacted]

Officer name: PH

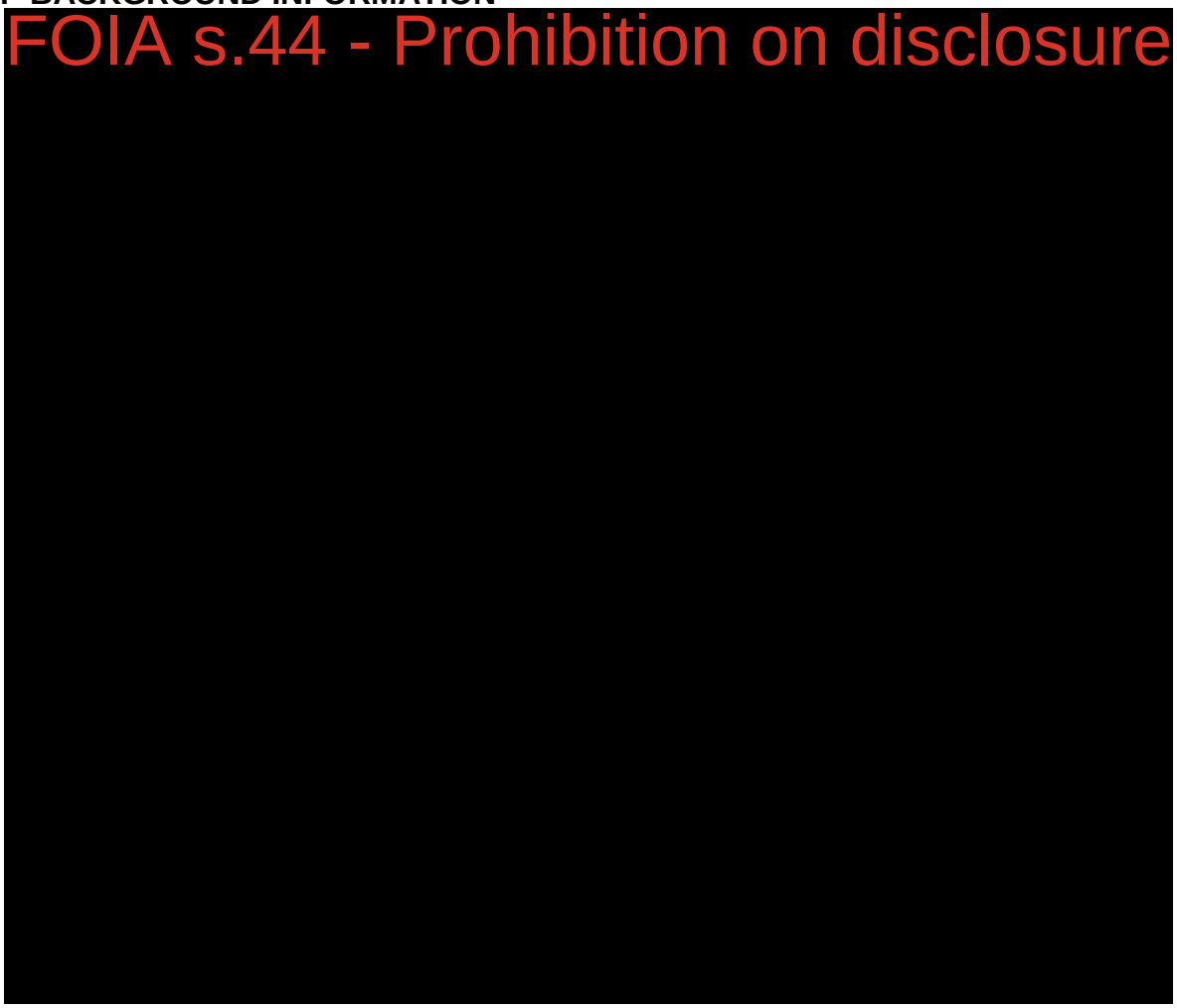
Officer Role: Head of the Locality Service

Date [redacted]

CONTENTS

1. **INTRODUCTION**
   A data breach has taken place on [redacted] resulting in confidential information contained in a number of court related documents being lost in public.

2. **BACKGROUND INFORMATION**



<u>The documents lost are:</u>

[redacted]

3. THE INCIDENT

[redacted] The Social worker left Court and put an envelope containing the documents on the top of her car and then drove off.

The Social Worker realising she had lost these when she got home and drove back, however was unable to locate the envelope containing the documents. The Social Worker also returned to the Court to establish if anyone has handed documents in from the car park.

4. DETAILS OF INVESTIGATION

- Requested and reviewed copies of the documents that made up the Court bundle that are missing to risk for any Data Breach.

- Manager has retraced the route the Social Worker took home from court to see if in the daylight the papers can be located possibly on the road or near to where she was parked. Manager also visited the court to discretely ask if any papers were handed in. The papers have not been recovered.

- Further checks of the nearby [redacted] undertaken. The Police will be informed about these missing documents in case a member of the public hand them in.

- Legal officers informed as the papers are documents of the court. Legal Services will alert us if the papers have been handed to them. Legal service where asked not to inform the other parties or the court until we have assessed the nature of the breach.

5. SUMMARY OF FINDINGS

- The document lost FOIA s.44 - Prohibition on disclosure [redacted]
- FOIA s.44 - Prohibition on disclosure [redacted]
- The Council in effect has lost court documents.
- Feedback from the manager for the case indicates Ealing were already under considerable criticism over its handling of the case. This was an initial hearing so will have implication for the Court team taking over case responsibility.

- FOIA s.44 - Prohibition on disclosure [redacted]

6. **RECOMMENDATIONS**
    - A management investigation into this breach has been instigated

---

Dear [redacted]

I write as a follow up to my email dated 3rd May 2016 in respect of Question 17 as below:-

Similarly, a9 from the audit report: ﷺLBE are currently trialling ﷺMetaComplianceﷺ policy management softwareﷺ and the action plan 20140120 a13; please confirm current status of the projected roll-out of March 2014.

Metacompliance has been successfully implemented within the organisation. A programme of disseminating policies is in place. The Data Protection Policy has been sent to all staff. I will forward separate to this email the statistics regarding training.

I have now been provided with further details regarding this and can advise you that since the beginning of 2016, there is a programme to review Information Governance policies and send them out by Metacompliance to all staff in the organisation. To date, we have reviewed the Acceptable Use Policy, Data Protection Policy and these have been sent out to all staff. The acceptance of these policies has been 100%, with the exception of staff who have not logged into the system due to long term absence.

The Information Security Policy is due to be sent out in the next two weeks and the Paper Handling Policy is currently out for review.

I trust this clarifies the situation but please do not hesitate to contact me if you have any further queries.

Yours sincerely

[redacted]

London Borough of Ealing

1 August 2016

Case reference number: COM0617270

Dear [redacted]

Please accept our apologies for the delay in responding to you. We are currently receiving a high volume of correspondence which has meant we have not been able to respond as promptly as we would wish.

Thank you for your response to my request for further information, received 3 May 2106.

However we have not yet been able to form a view on what action, if any, we will take as I need to seek clarification on several aspects around the incident in order to establish the facts further.

Therefore, to assist in my continuing investigation, I would be most grateful if you would provide the following information:

1. Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

2. With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

3. From the LBE Data Security Breach Report (05.02.16) Summary of Findings, final point [redacted]

FOIA s.44 - Prohibition on disclosure [redacted]

4. What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

5. What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Please provide the information requested by 13 August 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fall unde [redacted]
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

London Borough of Ealing

1 August 2016

Case reference number: COM0617270

Dear [redacted]

Please accept our apologies for the delay in responding to you. We are currently receiving a high volume of correspondence which has meant we have not been able to respond as promptly as we would wish.

Thank you for your response to my request for further information, received 3 May 2106.

However we have not yet been able to form a view on what action, if any, we will take as I need to seek clarification on several aspects around the incident in order to establish the facts further.

Therefore, to assist in my continuing investigation, I would be most grateful if you would provide the following information:

1. Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

2. With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

3. From the LBE Data Security Breach Report (05.02.16) Summary of Findings, final point [redacted]

4. What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

5. What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Please provide the information requested by 13 August 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fall und
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

Dear [redacted]

Thank you for your email received 1st August 2016 the contents of which have been noted.

I will provide the further information you have requested as soon as possible but no later than 13th August 2016.

Yours sincerely

[redacted] Corporate Information Governance Manager
[redacted]
✉ Ealing Council|Perceval House | 14-16 Uxbridge Road | 3rd Floor NE | Ealing | W5 2HL

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 01 August 2016 09:01
To: [redacted]
Subject: ICO - COM0617270 - Request for further information[Ref. COM0617270]

London Borough of Ealing

1 August 2016

Case reference number: COM0617270

Dear [redacted]

Please accept our apologies for the delay in responding to you. We are currently receiving a high volume of correspondence which has meant we have not been able to respond as promptly as we would wish.

Thank you for your response to my request for further information, received 3 May 2106.

However we have not yet been able to form a view on what action, if any, we will take as I need to seek clarification on several aspects around the incident in order to establish the facts further.

Therefore, to assist in my continuing investigation, I would be most grateful if you would provide the following information:

1. Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

2. With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

3. FOIA s.44 - Prohibition on disclosure [redacted]

4. What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

5. What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Please provide the information requested by 13 August 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fa [redacted]
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Contact us: 0303 123 1113, www.ico.org.uk, livechat and twitter @ICOnews

Dear [redacted],

I write further to your email received 1st August 2016 and our telephone conversation of today.

Please find the further information requested, with the exception of Question 4 , which will be sent to you by Friday 19th August 2016.

1)Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

Please see attached for your reference.

2)With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

In this incident the procedure detailed in the Paper Records Secure Handling and Transit Policy was not followed and therefore there is no approval request to provide.

FOIA s.44 - Prohibition on disclosure [redacted]

[redacted]

4)What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

I am awaiting the details regarding this question and I anticipate providing these to you by 19th August 2016.

5)What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

Staff within the Social Care directorate are required to complete the e-learn Data Protection training before they attend their line of business (FWi) system training. They need to provide their certificate to confirm they have completed the e-learn Data Protection course to their manager and the FWi trainers.

In addition, we currently perform quarterly checks on who has completed the programme using Itrent and eLearn (Corporate systems).

We also send our Data Protection policy to all staff via Metacompliance annually to remind them of their responsibilities.

Finally, if you have any further queries please do not hesitate to contact me.

Yours sincerely

FOIA s.44 - Prohibition on disclosure [redacted]
Corporate Information Governance Manager
[redacted]
ceval House | 14-16 Uxbridge Road | 3rd Floor NE | Ealing | W5 2HL

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 01 August 2016 09:01
To: [redacted]
Subject: ICO - COM0617270 - Request for further information[Ref. COM0617270]

London Borough of Ealing

1 August 2016

Case reference number: COM0617270

Dear [redacted]

Please accept our apologies for the delay in responding to you. We are currently receiving a high volume of correspondence which has meant we have not been able to respond as promptly as we would wish.

Thank you for your response to my request for further information, received 3 May 2106.

However we have not yet been able to form a view on what action, if any, we will take as I need to seek clarification on several aspects around the incident in order to establish the facts further.

Therefore, to assist in my continuing investigation, I would be most grateful if you would provide the following information:

1. Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

2. With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

3. FOIA s.44 - Prohibition on disclosure [redacted]

4. What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

5. What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Please provide the information requested by 13 August 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't re
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Contact us: 0303 123 1113, www.ico.org.uk, livechat and twitter @ICOnews

6 Recommendations

6.1 Recommendation 1

Management should review the findings in this report and consider any training or disciplinary issues that may be appropriate.

6.2 Recommendation 2

Advice and guidance contained in the “Paper Records Secure Handling and Transit Policy” should be updated and reviewed to ensure that it reflects social work practice and requirements. Details of the requirements should be widely circulated within social care and a link created in tri-x. Workers should be reminded of the principals of secure paper handling in the interim.

6.3 Recommendation 3

Specific guidance should be given to workers regarding the storage of confidential information at home. It should be made clear that, unless agreed storage is available, this is an exceptional circumstance. Documentation should be destroyed using council confidential waste facilities as soon as possible. A formal process for the provision of lockable home storage should be devised.

6.4 Recommendation 4

Each area office should have lockable cases available for workers who are required to transport papers out of the office. These should be kept securely and usage appropriately controlled.

6.5 Recommendation 5

Consideration should be given to providing SWs from localities teams with access to mobile working devices when attending court, in a similar way to that provided to the court team.

6.6 Recommendation 6

Roles and responsibilities for printing and transporting documents required as part of the court bundle should be clarified and confirmed with Legal. The outcome should be cascaded to social work teams.

6.7 Recommendation 7

All SC staff who have not yet completed e learning modules: Data Protection & Information Sharing and Confidentiality (Social Care), should be required to do so as soon as possible.

Dear [redacted]

I write further to your email received 1st August 2016 , my response dated 12th August 2016 and my subsequent telephone call to you last week.

Please find the further information requested in relation to Question 4.

4)What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

All new social care staff are required to complete the online data protection e-learning module in order to gain access to the social care line of business system. In addition Data Protection is an item on the Adults and Children's induction programme.

The Council has a number of social workers employed on a locum basis, as is the case for many local authorities, who do not form part of the corporate HR system to track online courses. In Ealing, locums make up 27% of the Children Services and have been informed of the online refresher training programme, however, these are not captured in the statistic of a 68% completion rate of permanent staff so far. This is not to say that locums have not completed the refresher training only that our HR systems are not able to capture it.

We are working towards 100% by the end of the year and delivering team-based refresher training sessions to include locum staff in the recording process.

Finally, if you have any further queries please do not hesitate to contact me.

Yours sincerely

[redacted] Corporate Information Governance Manager
[redacted]
✉ Ealing Council|Perceval House | 14-16 Uxbridge Road | 3rd Floor NE | Ealing | W5 2HL

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 01 August 2016 09:01
To: [redacted]
Subject: ICO - COM0617270 - Request for further information[Ref. COM0617270]

London Borough of Ealing

1 August 2016

Case reference number: COM0617270

Dear [redacted]

Please accept our apologies for the delay in responding to you. We are currently receiving a high volume of correspondence which has meant we have not been able to respond as promptly as we would wish.

Thank you for your response to my request for further information, received 3 May 2106.

However we have not yet been able to form a view on what action, if any, we will take as I need to seek clarification on several aspects around the incident in order to establish the facts further.

Therefore, to assist in my continuing investigation, I would be most grateful if you would provide the following information:

1. Please forward a copy of the Management Investigation mentioned in item 6 (RECOMMENDATIONS) of your Management Investigation Report dated 05.02.2016.

2. With reference to your Paper Records Secure Handling and Transit Policy section 2.1 line 3 and section 2.2: Please forward copies or details of the approval request and line manager approval for removal of the documents involved in this incident from the office and a copy of the log.

3. FOIA s.44 - Prohibition on disclosure [redacted]

4. What percentage of Social Care staff have now completed the refresher, on-line DP training detailed in your response 24 of 03.05.16 and what is the projected 100% completion date?

5. What mechanisms are in place to monitor completion of both mandatory initial DP training and refresher?

Your co-operation in providing full and detailed answers to our questions and establishing the facts is therefore appreciated.

If you have any further information relevant to this matter, including any additional remedial measures taken or changes to your policies, procedures or technical security, please provide full details when responding.

Further information and guidance relating to data security breach management is available on our website at:
http://www.ico.gov.uk/for_organisations/data_protection/lose.aspx

Please provide the information requested by 13 August 2016. If this will not be possible for some reason, or if you wish to discuss any aspect before responding, please contact me.

I look forward to hearing from you.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fa [redacted]
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

We are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the Data Protection Act 1998 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk). Please say whether you consider any of the information you send us is confidential. You should also say why. We will only withhold information where there is good reason to do so.

The ICO's mission is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Contact us: 0303 123 1113, www.ico.org.uk, livechat and twitter @ICOnews

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policies. These refer to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider…LBE policies such as those covering secure data handling/transportation…". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The 100% target completion of mandatory, online data protection refresher training for all Social Care staff is achieved by 1 February 2017. This to include locum and other temporary staff whose roles require the handling of personal data. That the same monitoring and recording processes are applied to this latter group as that of permanent staff.

(2) Also that both initial and refresher data protection related training recording and monitoring of non-permanent staff employed in all departments of the council involved in the handling of personal data is included in completion measurement and verification.
To ensure the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(3) The ICO notes the LBE Management Investigation Report Recommendations made and approve of the following as preventative measures:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 1 February 2017.

b) That availability of lockable cases in each area office is completed by 1 February 2017 and that similar

arrangements are made in all council departments where removal of similar documents from the office is a requirement.

c) That the review of making home working electronic devices for all social workers is completed with recommendations made by 1 February 2017.

d) That the review with Legal with regard to roles and responsibilities for printing and transporting documents required as part of court bundles is completed with recommendations made by 1 February 2017.

e) That, where changes result from a) and b) above, staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained by 1 February 2017 in how to follow that policy.

(4) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement

For and on behalf of the Information Commissioner

Dated: …….

Good afternoon [redacted]

Could you please confirm which of these two addresses is correct for the Chief Executive's office:

Perceval House, 14-16 New Broadway, Ealing. W5 4HL

or

Perceval House, 14/16 Uxbridge Road, London. W5 2HL

Please also confirm that Paul Najsarek is our current Chief Exec.

Thank you.

[redacted]
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Dear [redacted]

Thank you for your email.

The correct address is :

Perceval House, 14/16 Uxbridge Road, London. W5 2HL

I confirm that Paul Najsarek is our current Chief Executive.

Yours sincerely

[redacted] Corporate Information Governance Manager
[redacted]
✉ Ealing Council|Perceval House | 14-16 Uxbridge Road | 3rd Floor NE | Ealing | W5 2HL

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 02 September 2016 15:22
To: [redacted]
Subject: ICO - COM0617270 - Confirmation of address[Ref. COM0617270]

Good afternoon [redacted]

Could you please confirm which of these two addresses is correct for the Chief Executive's office:

Perceval House, 14-16 New Broadway, Ealing. W5 4HL

or

Perceval House, 14/16 Uxbridge Road, London. W5 2HL

Please also confirm that Paul Najsarek is our current Chief Exec.

Thank you.

[redacted]
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider…LBE policies such as those covering secure data handling/transportation…". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their stated target for 100% completion of mandatory, online data protection refresher training for all Social Care staff and that this is achieved by 1 February 2017. This to include locum and other temporary staff whose roles require the handling of personal data. That the same monitoring and recording processes are applied to this latter group as that of permanent staff.

(2) Both initial and refresher data protection related training recording and monitoring of non-permanent staff employed in all departments of the council involved in the handling of personal data is included in completion measurement and verification.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are welcomed by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 1 February 2017.

b) That, where changes result from the above, staff are made aware, via MetaCompliance or similar, of the Council's revised policy for the secure handling and transit of personal data and this policy forms part of future data protection training programs where appropriate.

c) That availability of lockable cases in each area office is completed by 1 February 2017 and that similar arrangements are made in all council departments where removal of similar documents from the office is a requirement.

d) That the review of providing Social Workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 1 February 2017.

e) That the review with the Legal Social Care and Education Department regarding roles and responsibilities for printing and transporting documents required as part of court bundles is completed with recommendations made by 1 February 2017.

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

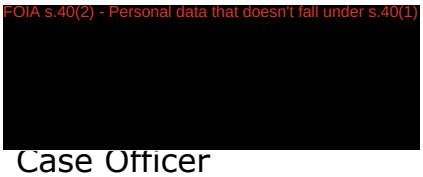
Dated: …….

Good afternoon JP,

Re.: London Borough of Ealing - COM0617270

Could you please review the attached undertaking. Do you think the targets set and the tasks described are reasonable, achievable and measurable as a follow-up?

I look forward to your comments.



Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Logo

FOIA s.40(2) - Personal data that doesn't fall under s.40(1

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn @ico.gsi.gov.uk

From: Christine Eckersley
Sent: 23 September 2016 10:00
To: FOIA s.40(2) - Personal data that do
Subject: London Borough of Ealing Undertaking - COM0617270

Hi FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Draft u/t attached with comments - if any queries, re comments / amendments please let me know.

We will log receipt of this - the u/t follow up is officially assigned to an auditor once we receive a copy of the organisation's agreed & signed u/t. At that time, we will also need confirmation of the council's named key contact for the undertaking follow up.

Thanks

Logo

Christine Eckersley
Team Manager

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545731 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
christine.eckersley@ico.gsi.gov.uk

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider…LBE policies such as those covering secure data handling/transportation…". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their target for 100% completion of mandatory, online data protection refresher training for all Social Care staff and that this is achieved by 1 February 2017. This to include locum and other temporary staff whose roles require the handling of personal data. That the same monitoring and recording processes are applied to this latter group as that of permanent staff.

(2) Both initial and refresher data protection related training recording and monitoring of non-permanent staff employed in all departments of the council involved in the handling of personal data is included in completion measurement and verification.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are approved by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 1 February 2017.

b) That availability of lockable cases in each area office is completed by 1 February 2017 and that similar arrangements are made in all council departments where removal of similar documents from the office is a requirement.

c) That the review of making home working electronic devices for all social workers is completed with recommendations made by 1 February 2017.

d) That the review with Legal with regard to roles and responsibilities for printing and transporting documents required as part of court bundles is completed with recommendations made by 1 February 2017.

e) That, where changes result from a) and b) above, staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained by 1 February 2017 in how to follow that policy.

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….

Good afternoon [redacted]

Re.: COM0617270

I tried to telephone you but your unmonitored voicemail has the message that you are not in the office until 19th September hence the email.

My case recommendations are currently with our Good Practice department for review. They have asked for clarification on the LBE recommendation No. 6: "Roles and responsibilities for printing and transporting documents required as part of the court bundle should be clarified and confirmed with Legal. The outcome should be cascaded to social work teams."

Could you please confirm the full department title referred to above as 'Legal'.

Thank you.

[redacted]
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Dear [redacted]

Thank you for your email.

The department concerned is Legal Social Care and Education.

I hope this clarifies but if you have any further queries please do not hesitate to contact me.

Yours sincerely

[redacted] | Corporate Information Governance Manager
[redacted]
✉ Ealing Council|Perceval House | 14-16 Uxbridge Road | 3rd Floor NE | Ealing | W5 2HL

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 26 September 2016 14:09
To: [redacted]
Subject: ICO - COM0617270 - Clarification point[Ref. COM0617270]

Good afternoon [redacted]

Re.: COM0617270

I tried to telephone you but your unmonitored voicemail has the message that you are not in the office until 19th September hence the email.

My case recommendations are currently with our Good Practice department for review. They have asked for clarification on the LBE recommendation No. 6: "Roles and responsibilities for printing and transporting documents required as part of the court bundle should be clarified and confirmed with Legal. The outcome should be cascaded to social work teams."

Could you please confirm the full department title referred to above as 'Legal'.

Thank you.

[redacted]
Case Officer
The Information Commissioner's Office

Direct telephone 01625 545300

Hello again Christine,

I understand you are in thick of it at the moment so, when it is next convenient to you:

Re.: London Borough of Ealing COM0617270 Undertaking.

I have reworded and restructured recommendation 4 a-e hopefully in line with the advice you gave. Is this now more in line with facilitating follow-up requirements?

Now includes clarification on the department title referred to as 'Legal'.

Thank you

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Case Officer
The Information Commissioner’s Office
Direct telephone 01625 545300

Hi [redacted]

Currently QA'ing E. Dunbartonshire for report issue next week, but will look at it in next couple of days -prob first thing Weds am– if any probs, just let me know.

Thanks.

Logo

Christine Eckersley
Team Manager

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545731 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
christine.eckersley@ico.gsi.gov.uk

From: casework@ico.org.uk [mailto:casework@ico.org.uk]
Sent: 26 September 2016 15:47
To: Christine Eckersley
Subject: London Borough of Ealing COM0617270 Undertaking V3 with GP recommendations [Ref. COM0617270]

Hello again Christine,

I understand you are in thick of it at the moment so, when it is next convenient to you:

Re.: London Borough of Ealing COM0617270 Undertaking.

I have reworded and restructured recommendation 4 a-e hopefully in line with the advice you gave. Is this now more in line with facilitating follow-up requirements?

Now includes clarification on the department title referred to as 'Legal'.

Thank you

[redacted]
Case Officer
The Information Commissioner's Office

Direct telephone 01625 545300

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider…LBE policies such as those covering secure data handling/transportation…". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their stated target for 100% completion of mandatory, online data protection refresher training for all permanent, locum and temporary Social Care staff who handle personal data by 3 April 2017. That the same monitoring and recording processes for the completion of this training are applied to those locum, temporary and permanent social care staff.

(2) The Recording and monitoring of initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data is performed as (1) above.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are welcomed by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 3 April 2017.

b) That, where changes result from the above, staff are made aware, via MetaCompliance or similar, of the Council's revised policy for the secure handling and transit of personal data and this policy forms part of future data protection training programmes where appropriate.

c) That availability of lockable cases in each area office is completed by 3 April 2017 and that similar arrangements are made in all council departments where removal of similar documents containing personal data from the office is a requirement.

d) That the review of providing Social Workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 3 April 2017.

e) That the review with the Legal Social Care and Education Department, regarding roles and responsibilities for printing and transporting documents required as part of court bundles, is completed with recommendations made by 3 April 2017.

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….

FAO Mr. Paul Najsarek, Chief Executive

Ealing Council
Perceval House,
14/16 Uxbridge Road,
London.
W5 2HL

4 October 2016

Case reference number: COM0617270

Dear Mr Najsarek

I refer to the above matter, which has been investigated by the Information Commissioner's Office (ICO).

As you will be aware, a Social Worker FOIA s.44 - Prohibition on disclosure [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents which have not been recovered.

Given the above factors, the ICO considers it likely that London Borough of Ealing, as data controller, has breached the 7th principle of the Data Protection Act (the 'Act') which states that:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Having taken into account the specific circumstances of this incident and the remedial actions taken, we are satisfied that it is not necessary for us to take any form of enforcement action at this stage subject to London Borough of Ealing agreeing to an undertaking (enclosed) which sets out the steps the Commissioner

to be taken to reduce the chances of similar incidents occurring in the future.

I would therefore be grateful if Mr. Paul Najsarek, Chief Executive of London Borough of Ealing would sign and return the undertaking to me by 20 October 2016 unless London Borough of Ealing wishes to raise an issue of substance with regard to the wording which it would like to be considered by the ICO.

On its return, the undertaking will be signed by the ICO's Head of Enforcement and the text will be published on our website. We may also publicise this. A copy of the signed document will then be returned to you for your records. You should note that any breach of a signed undertaking would be more likely to lead to enforcement action being taken by the ICO.

Further, we would also expect London Borough of Ealing to agree that the ICO may follow up the undertaking to gain assurance that the agreed actions have been implemented and embedded within six months of the undertaking being signed.

If you have any queries about the undertaking, please do not hesitate to contact me. Otherwise, I look forward to hearing from you by 20 October 2016.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fall unde
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

Good morning,

Re.: Undertaking - London Borough of Ealing - COM0617270

He attached undertaking has now been reviewed by good practice and is ready to be forwarded to the DC for their comments before signing.

I believe it is at this stage the press office are informed to evaluate whether it will be of interest to you?

Best regards

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn't @ico.gsi.gov.uk

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider…LBE policies such as those covering secure data handling/transportation…". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their stated target for 100% completion of mandatory, online data protection refresher training for all permanent, locum and temporary Social Care staff who handle personal data by 3 April 2017. That the same monitoring and recording processes for the completion of this training are applied to those locum, temporary and permanent social care staff.

(2) The Recording and monitoring of initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data is performed as (1) above.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are welcomed by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 3 April 2017.

b) That, where changes result from the above, staff are made aware, via MetaCompliance or similar, of the Council's revised policy for the secure handling and transit of personal data and this policy forms part of future data protection training programmes where appropriate.

c) That availability of lockable cases in each area office is completed by 3 April 2017 and that similar arrangements are made in all council departments where removal of similar documents containing personal data from the office is a requirement.

d) That the review of providing Social Workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 3 April 2017.

e) That the review with the Legal Social Care and Education Department, regarding roles and responsibilities for printing and transporting documents required as part of court bundles, is completed with recommendations made by 3 April 2017.

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….

Good morning [redacted]

Re.: Our Case Reference COM0617270

For your information:

When I wrote to you on 24 March 2016, I set out details of the Information Commissioner's powers. Based on the information you have provided, we have decided that regulatory action is not required in this case.

However, we will shortly be issuing an undertaking which will be posted to your Chief Executive with a copy emailed to you. The covering letter will be self-explanatory.

Best regards

[redacted]
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Re.: COM0617270

Good afternoon [redacted]

For your information:

Please find attached, copy of Undertaking and covering letter which will be going by tomorrow's post addressed to Paul Najsarek.

Best regards

[redacted]
Case Officer
The Information Commissioner’s Office
Direct telephone 01625 545300

From: ChiefExecutive [mailto:ChiefExecutive@ealing.gov.uk]
Sent: Tuesday, October 11, 2016 5:37 PM
To: casework
Subject: Case reference COM0617270

Dear [redacted]

Further to your letter which was received yesterday, Mr Najsarek has now signed the undertaking you provided and we are returning it to you by Special Delivery today.

I attach a scanned copy for your records.

Kind regards,

[redacted]

Complaints and Admin Officer
Chief Executive's Office

www.mimecast.com

****

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. FOIA s.44 - Prohibition on disclosure February 2016, a Social Worker attended Court regarding care proceedings FOIA s.44 - Prohibition on disclosure FOIA s.44 - Prohibition on disclosure She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider...LBE policies such as those covering secure data handling/transportation...". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their stated target for 100% completion of mandatory, online data protection refresher training for all permanent, locum and temporary Social Care staff who handle personal data by 3 April 2017. That the same monitoring and recording processes for the completion of this training are applied to those locum, temporary and permanent social care staff.

(2) The Recording and monitoring of initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data is performed as (1) above.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are welcomed by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 3 April 2017.

b) **That, where changes result from the above, staff are made aware, via MetaCompliance or similar, of the Council's revised policy for the secure handling and transit of personal data and this policy forms part of future data protection training programmes where appropriate.**

c) **That availability of lockable cases in each area office is completed by 3 April 2017 and that similar arrangements are made in all council departments where removal of similar documents containing personal data from the office is a requirement.**

d) **That the review of providing Social Workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 3 April 2017.**

e) **That the review with the Legal Social Care and Education Department, regarding roles and responsibilities for printing and transporting documents required as part of court bundles, is completed with recommendations made by 3 April 2017.**

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: P. Najsarek

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: 10/10/16.

Signed: .....

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: .....

FAO Mr. Paul Najsarek, Chief Executive

Ealing Council

21 October 2016

Case reference number: COM0617270

Dear Mr Najsarek

Thank you for returning the signed Undertaking.

My apologies for the delay in acknowledging, [redacted].

Unfortunately the Head of Enforcement, Stephen Eckersley, is out of the country at the present time undertaking international obligations and will not return until 28 October 2016.

I shall ask him to countersign the Undertaking on his return and forward a copy to you.

This delay, of course, will be reflected in our publication date and also that of the follow-up date.

Yours sincerely

[redacted]
Case Officer
Information Commissioner's Office
01625 545300 direct dial telephone number

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted] She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered the fact that some of the data lost in this incident consisted of information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider...LBE policies such as those covering secure data handling/transportation...". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the Paper Records Secure Handling and Transit Policy could either be reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their stated target for 100% completion of mandatory, online data protection refresher training for all permanent, locum and temporary Social Care staff who handle personal data by 3 April 2017. That the same monitoring and recording processes for the completion of this training are applied to those locum, temporary and permanent social care staff.

(2) The Recording and monitoring of initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data is performed as (1) above.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are welcomed by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 3 April 2017.

b) That, where changes result from the above, staff are made aware, via MetaCompliance or similar, of the Council's revised policy for the secure handling and transit of personal data and this policy forms part of future data protection training programmes where appropriate.

c) That availability of lockable cases in each area office is completed by 3 April 2017 and that similar arrangements are made in all council departments where removal of similar documents containing personal data from the office is a requirement.

d) That the review of providing Social Workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 3 April 2017.

e) That the review with the Legal Social Care and Education Department, regarding roles and responsibilities for printing and transporting documents required as part of court bundles, is completed with recommendations made by 3 April 2017.

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: P. Najsarek

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: 10/10/16.

Signed: .....

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: 31 OCTOBER 2016

Chief Executive

Ealing
www.ealing.gov.uk

Ealing Council
Perceval House
14-16 Uxbridge Road
London W5 2HL

t 020 8825 5000

BY SPECIAL DELIVERY

Mr P Harrison,
Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

11 October 2016

Dear [redacted]

Re: Case reference number:COM0617270

I refer to your letter dated 4 October to Mr Najsarek, the Chief Executive, which was received yesterday.

Mr Najsarek has signed the enclosed undertaking and I now return it to you as requested.

Yours sincerely,

[redacted]

Complaints and Admin Officer
Chief Executive's Office

t 020 8825 5000

Logo

[redacted]

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
[redacted]@ico.gsi.gov.uk

From: [redacted]
Sent: 02 November 2016 09:45
To: [redacted]
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Good morning [redacted]

I hope that you are well.

We have now received the signed Ealing Council undertaking and Steve Eckersley (after his international sojourn) has also now signed it. There were no changes requested by the DC so the original copy I sent when I first notified you still stands. Not sure whether you also need the signed copy so I have attached it just in case.

[redacted]

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
[redacted]@ico.gsi.gov.uk

From: [redacted]
Sent: 10 October 2016 11:37

To: [redacted]
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Thanks [redacted] I'll start work on a draft press release and if you could let me know when the final version of the undertaking is signed and ready to be publicised we'll go ahead then.

Thanks

[redacted]
Lead Communications Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545345 F. 01625 524510 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

From: [redacted]
Sent: 04 October 2016 09:05
To: [redacted]
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Good morning [redacted]

I shall be sending the draft U/T to the DC today. They, of course, will have the opportunity to either accept and sign or challenge some of the requirements. I would think that, at the latest, this would be completed within a couple of weeks.

If they challenge, then it will be a how long is a piece of string moment. However, I don't anticipate any significant issues to be raised so I would think the whole process will be 2-3 weeks.

[redacted] but I don't think that will present any problems with the process.

[redacted]
Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn't @ico.gsi.gov.uk

From: FOIA s.40(2) - Personal data that
Sent: 03 October 2016 15:17
To: FOIA s.40(2) - Personal data that d
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Hi FOIA s.40(2) - Personal data that doesn't fall u

I've had a quick read and we'd like to do a press release with this. What sort of timescales do you think we're looking at for when we'd be putting this on the website? I'll write a press release to co-inside.

Many thanks

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)
Lead Communications Officer
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545345 F. 01625 524510 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

From: FOIA s.40(2) - Personal data that d
Sent: 03 October 2016 08:39
To: Press Team (internal)
Cc: casework
Subject: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Good morning,

Re.: Undertaking - London Borough of Ealing - COM0617270

He attached undertaking has now been reviewed by good practice and is ready to be forwarded to the DC for their comments before signing.

I believe it is at this stage the press office are informed to evaluate whether it will be of interest to you?

Best regards

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Case Officer

Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn't @ico.gsi.gov.uk

Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

2 November 2016

Case reference number: COM0617270

By email only to: FOIA s.44 - Prohibition on disclosure

Dear FOIA s.44 - Prohibition on disclosure

Thank you for agreeing to the requirements of the undertaking in relation to the above case. I enclose a copy of the signed undertaking for the London Borough of Ealing's records. With the signing of the undertaking the above case is now closed.

An unsigned copy of the undertaking will shortly be published on the ICO's website and we may issue a press release to accompany this.

The London Borough of Ealing will be contacted by the ICO's Good Practice department in due course to arrange a follow-up to the undertaking to assess the action that has been taken to meet the undertaking's requirements.

Yours sincerely

FOIA s.40(2) - Personal data that doesn't fall
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Logo

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn @ico.gsi.gov.uk

From: FOIA s.40(2) - Personal data that do
Sent: 02 November 2016 10:09
To: Christine Eckersley
Subject: FW: Signed UT Ealing - CONTACT DETAILS OMITTED

Hello again Christine!

Just occurred to me that I forgot to give you the contact details for Ealing.

The FOIA s.44 - Pro I have been dealing with is:

FOIA s.44 - Prohibition on disclosure Corporate Information Governance Manager)
Tel: FOIA s.44 - Prohibition on disclosure
Email: FOIA s.44 - Prohibition on disclosure

FOIA s.40(2) - Personal data that doesn't fall under s

Logo

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn @ico.gsi.gov.uk

From: [redacted]
Sent: 02 November 2016 09:54
To: Christine Eckersley
Subject: RE: Ealing u/t V.03

Good morning Christine,

Re.: Signed Undertaking, Ealing Council

Steve (following his jollies abroad!) has now signed the undertaking which is attached.

As there was some delay in getting it signed, following its return from the DC, I assume that an allowance will be made on the follow-up date on that originally stated and agreed?

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
[redacted]@ico.gsi.gov.uk

From: Christine Eckersley
Sent: 29 September 2016 09:46
To: [redacted]
Subject: RE: Ealing u/t V.03

Hi [redacted]

Thanks for the update. We don't have involvement in the press office side of u/t's, so can't advise on that.

As suggested amendments agreed, you could just forward me a copy of the u/t email to the council for our records.

Re my previous comments, once the council have signed and agreed the u/t, you'll need to forward signed copy, confirm their 'key contact' for the u/t activity, and I'll then allocate to an auditor/put in planner.

Thanks.

Logo

Christine Eckersley
Team Manager

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545731 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
christine.eckersley@ico.gsi.gov.uk

From: [redacted]
Sent: 29 September 2016 09:38
To: Christine Eckersley
Subject: RE: Ealing u/t V.03

Morning Christine,

Thanks for reviewing the U/T. I agree, on re-reading the U/T as submitted, those sections were somewhat cumbersome. Your suggestions provide clarity and make the recommendations more succinct.

I have now incorporated the amendments and will submit the document prior to sending to the council.

I believe I should now pass this to the press office so they can evaluate whether it will be of interest?

[redacted]

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
[redacted]@ico.gsi.gov.uk

From: Christine Eckersley
Sent: 28 September 2016 17:07
To: [redacted]
Subject: Ealing u/t V.03

Hi [redacted]

I've had another look at this – thanks for the correction/amendments.

The u/t reccs 1 and 2 are a little complex in structure so I've amended to make the content clearer (in theory!)

Let me know if you want to discuss amended content. Otherwise, can you send me a finalised copy of the u/t prior to issue to the Council.

Thanks

Logo

Christine Eckersley
Team Manager

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545731 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
christine.eckersley@ico.gsi.gov.uk

London Borough of Ealing

2 November 2016

Case Ref.: COM0617270

Good morning [redacted]

Please find attached, case closure letter and a copy of the dual signature undertaking.

Thank you for your co-operation during the investigation of this case.

Best regards

[redacted]
Case Officer
The Information Commissioner’s Office
Direct telephone 01625 545300

ICO Ref: **COM0617270**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: London Borough of Ealing

Ealing Council
Perceval House
14/16 Uxbridge Road
London
W5 2HL

I, Paul Najsarek, Chief Executive of the London Borough of Ealing, for and on behalf of the London Borough of Ealing hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The London Borough of Ealing is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by the London Borough of Ealing and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was informed by the London Borough of Ealing on 18 February 2016 of the loss of a court bundle containing personal and sensitive personal data relating to 27 data subjects including 14 children.

3. [redacted] February 2016, a Social Worker attended Court regarding care proceedings [redacted]. She left Court, put an envelope containing the documents on the top of her car and then drove off. When she got home she realised that she did not have the documents. Despite searching the car park, the social worker's route home and making enquiries locally, the documents have not been recovered to date.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

I to the Act. The Commissioner has also considered that some of the data lost in this incident consisted information as to the physical or mental health or condition of some of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2[(e)] of the Act.

5. It is acknowledged that the council has submitted mitigating factors with regard to this incident. Training had been given to and completed by the individual involved and suitable procedures were in place.

6. However, during the Commissioner's investigation of the incident she was advised by the council that as of 19 August 2016, only 68% of permanent staff within Social Care had completed refresher Data Protection training. This figure does not include the 27% of staff within Children's services made up of locums. The council are therefore unable to determine if those locums have completed refresher training from records held.

7. On 13-15 May 2013 the Commissioner conducted an audit of the data controller's data protection compliance, in which the lack of mandated, periodic data protection related refresher training was highlighted. The Commissioner's recommendation was accepted by the council and stated: "Annual DP e-learning refresher training to be rolled out in March 2014 with the use of MetaCompliance." The audit was followed up on 18 March 2014, and it was suggested that this outstanding action should be prioritised for completion.

8. During the investigation, the Commissioner was also informed that no records were available relating to the requirements of the council's 'Paper Records Secure Handling and Transit' policy. This refers to the requirement for a management approval request to be made for removal of documents from the council's office and that, having been granted consent, document details are entered into in the office log for reference in case of loss. The Commissioner was also made aware that secure lockable cases had previously been made available but were no longer so.

9. During the audit carried out by the Commissioner in 2013, a recommendation was made that "Self-assessments should consider...LBE policies such as those covering secure data handling/transportation...". With this in mind and given certain aspects of the incident revealed during this investigation, the

manager's role in implementing and enforcing the P. Records Secure Handling and Transit Policy could eit reviewed or reinforced and that training gaps are identified and, if required, corrected.

10. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) The council continue to work toward achieving their stated target for 100% completion of mandatory, online data protection refresher training for all permanent, locum and temporary Social Care staff who handle personal data by 3 April 2017. That the same monitoring and recording processes for the completion of this training are applied to those locum, temporary and permanent social care staff.

(2) The Recording and monitoring of initial and refresher data protection training for non-permanent staff employed in all other departments of the council involved in the handling of personal data is performed as (1) above.

(3) The council ensures the use of MetaCompliance is a sufficiently robust mechanism for delivering and measuring refresher DP related training to meet the council's stated objective of an annual requirement.

(4) The LBE Management Investigation Report Recommendations, which are welcomed by the Commissioner, are progressed as follows:

a) The review and, if found to be necessary, implementation of an updated Paper Records Secure Handling and Transit Policy is completed by 3 April 2017.

b) That, where changes result from the above, made aware, via MetaCompliance or simil Council's revised policy for the secure handling and transit of personal data and this policy forms part of future data protection training programmes where appropriate.

c) That availability of lockable cases in each area office is completed by 3 April 2017 and that similar arrangements are made in all council departments where removal of similar documents containing personal data from the office is a requirement.

d) That the review of providing Social Workers from localities teams with access to mobile working devices when attending court is completed with recommendations made by 3 April 2017.

e) That the review with the Legal Social Care and Education Department, regarding roles and responsibilities for printing and transporting documents required as part of court bundles, is completed with recommendations made by 3 April 2017.

(5) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: .....

Paul Najsarek
Chief Executive
London Borough of Ealing

Dated: .....

Signed: .....

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: .....

15 November 2016

Case Reference Number COM0617270

Dear [redacted]

I am writing with regard to the telephone conversation I had with [redacted] last Thursday (10.10.16) in which, I believe, you were also present.

We discussed the possibility of amending the Undertaking to remove information that could possibly identify the family involved. The conclusion at that time was to amend the document and forward it for resigning.

We have, however, decided that this will not be necessary. The Undertaking will be published on the website as a redacted document and I attach a copy for your information.

Yours sincerely,

[redacted]
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Good afternoon [redacted]

Just letting you know that both the press release and the undertaking have now been posted on our website; in case the council would like to respond.

Best regards

[redacted]
Case Officer
The Information Commissioner's Office
Direct telephone 01625 545300

Logo

[redacted]

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
[redacted]@ico.gsi.gov.uk

From: [redacted]
Sent: 02 November 2016 16:28
To: [redacted]
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Hi [redacted]

We've just had a quick chat in the press office about press releases coming up. We've got quite a lot so we're going to meet on Friday to work out timings for them all.

Are you OK to hold off the web form until then? I'm thinking possibly the week after next for the undertaking press release but will let you know on Friday.

Thanks

[redacted]

Lead Communications Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545345 F. 01625 524510 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

From: [redacted]
Sent: 02 November 2016 09:45
To: [redacted]
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Good morning [redacted]

I hope that you are well.

We have now received the signed Ealing Council undertaking and Steve Eckersley (after his international sojourn) has also now signed it. There were no changes requested by the DC so the original copy I sent when I first notified you still stands. Not sure whether you also need the signed copy so I have attached it just in case.

[redacted]

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
[redacted]@ico.gsi.gov.uk

From: [redacted]
Sent: 10 October 2016 11:37
To: [redacted]
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Thanks [redacted] I'll start work on a draft press release and if you could let me know when the final version of the undertaking is signed and ready to be publicised we'll go ahead then.

Thanks

[redacted]

Lead Communications Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545345 F. 01625 524510 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

From: FOIA s.40(2) - Personal data that do
Sent: 04 October 2016 09:05
To: FOIA s.40(2) - Personal data tha
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Good morning FOIA s.40(2) - Personal data that doesn't fall und

I shall be sending the draft U/T to the DC today. They, of course, will have the opportunity to either accept and sign or challenge some of the requirements. I would think that, at the latest, this would be completed within a couple of weeks.

If they challenge, then it will be a how long is a piece of string moment. However, I don't anticipate any significant issues to be raised so I would think the whole process will be 2-3 weeks.

FOIA s.40(2) - Personal data that doesn't fall under s.40(1) but I don't think that will present any problems with the process.

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn @ico.gsi.gov.uk

From: FOIA s.40(2) - Personal data tha
Sent: 03 October 2016 15:17
To: FOIA s.40(2) - Personal data that do
Subject: RE: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Hi FOIA s.40(2) - Personal data that doesn

I've had a quick read and we'd like to do a press release with this. What sort of timescales do you think we're looking at for when we'd be putting this on the website? I'll write a press release to co-inside.

Many thanks

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Lead Communications Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545345 F. 01625 524510 ico.org.uk twitter.com/iconews
Please consider the environment before printing this email

From: FOIA s.40(2) - Personal data that do
Sent: 03 October 2016 08:39
To: Press Team (internal)
Cc: casework
Subject: Undertaking - London Borough of Ealing - [Ref. COM0617270]

Good morning,

Re.: Undertaking - London Borough of Ealing - COM0617270

He attached undertaking has now been reviewed by good practice and is ready to be forwarded to the DC for their comments before signing.

I believe it is at this stage the press office are informed to evaluate whether it will be of interest to you?

Best regards

FOIA s.40(2) - Personal data that doesn't fall under s.40(1)

Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
T. 01625 545300 F. 01625 524510 ico.org.uk
twitter.com/iconews
Please consider the environment before printing this email
For secure emails over gsi please use
FOIA s.40(2) - Personal data that doesn @ico.gsi.gov.uk