Data protection

Findings from ICO audits of 16 local authorities

January to December 2013

Information Commissioner's Office

Introduction

This report is based on ICO audits of **16 local authorities** between January and December 2013. This report highlights our experience of personal data handling by those organisations and is intended to help them, and others in the sector, see where they can make improvements in how they handle personal data. No individual organisation is named in this report.

We carry out **risk assessments** to ensure that we target our limited audit resources to those organisations which we believe would most benefit from working with us, namely those which are likely to have a basic understanding about complying with the Data Protection Act 1998 (the DPA) and to have some associated policies and procedures in place, but would benefit from focused assistance in meeting their obligations.

In addition, we monitor the **trends** logged by the Enforcement Department of the ICO in determining which organisations we offer the opportunity to participate in our audit programme:

- ICO Enforcement Trends.

In January 2012, the Information Commissioner wrote in conjunction with the Permanent Secretary for the **Department for Communities and Local Government** to all local authority Chief Executives, outlining some key information governance requirements and encouraging participation in our audit programme:

- ICO & DCLG letter.

In December 2013, the Information Commissioner wrote in conjunction with the Chairman of the **Local Government Association** to all council leaders, reiterating the commitment of both to work with local authorities to improve their data protection compliance, but highlighting the fact that the ICO would have to seek further powers to undertake compulsory audits of local authorities if standards did not improve sufficiently during 2014:

- ICO & LGA letter.

Assurance ratings

When conducting an audit, we assess the arrangements that an organisation has in place for complying with the Data Protection Act 1998 (DPA) and the extent to which they are adhering to them.

We then give an overall 'assurance rating' (as described below) indicating the extent to which controls are in place and are effective.

Assurance rating	Description
High assurance	Limited scope for improving existing arrangements. Significant action unlikely to be required.
Reasonable assurance	Some scope for improvement in existing arrangements.
Limited assurance	Considerable scope for improvement in existing arrangements.
Very limited assurance	Substantial risk of non-compliance with DPA. Immediate action required.

Overall audit assurance ratings

During the period, we audited 16 local authorities and gave the following overall assurance ratings:

Audits completed	High assurance	Reasonable assurance	Limited assurance	Very limited assurance
16	0	9	6	1

- 0% fell within the high assurance range.
- 56% fell within the reasonable assurance range.
- 38% fell within the limited assurance range.
- 6% fell within the very limited assurance range.

This clearly shows there is room for improvement in all the organisations we visited.

Scope area assurance ratings

We usually cover three of the six key scope areas described below and give an assurance rating in each of the individual scope areas we audit.

Each scope area contains within it a number of specific controls. We individually score each control to provide the assurance rating for the scope area being assessed. Where we identify information risks within a scope area, we make recommendations to mitigate these and increase assurance against specific controls.

During the period, we gave the following assurance ratings in each scope area:

Scope area	Rating	Total
Data protection governance The arrangements and controls in place to ensure compliance with the DPA.	High	0
	Reasonable	2
	Limited	3
	Very limited	1
Records management The processes in place for managing electronic and manual records containing personal data.	High	0
	Reasonable	7
	Limited	3
	Very limited	2
Requests for personal data The procedures in place to deal with any requests for personal	High	0
	Reasonable	3

data.	Limited	1
	Very limited	0
Security of personal data The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.	High	0
	Reasonable	6
	Limited	3
	Very limited	0
Training and awareness The provision and monitoring of staff DPA training and the awareness of DPA requirements relating to their roles and responsibilities.	High	1
	Reasonable	3
	Limited	2
	Very limited	3
Data sharing The design and operation of controls to ensure the sharing of personal data complies with the principles of the DPA and the Information Commissioner's Data Sharing Code of Practice.	High	0
	Reasonable	4
	Limited	1
	Very limited	0

Areas of good practice

We observed good practice in the following areas (though these should not be viewed as representative of our audit findings as a whole).

Data protection governance

✓ The organisation **assigns ownership** of information governance to key posts, for example, a Data Protection Officer (DPO) and a Senior Information Risk Owner (SIRO).

Case study

A council has a SIRO who sits on the Corporate Management Board (CMB), the data protection steering group, the information security steering group and a further data protection improvement group for key managers. The DPO chairs both the data protection and improvement steering groups.

The council has a Caldicott Guardian and nominated Information Asset Owners (IAOs). All senior managers have a clear understanding of data protection issues and review them at regular management meetings.

✓ The organisation **publishes** and makes policies and procedures available to all employees to promote awareness of their corporate responsibilities in relation to data protection compliance.

Case study

A council publishes its data protection policies on the intranet, and uses a policy management software tool to record when staff have read and accepted them. The council communicates any changes to policies to staff using a variety of methods, including the intranet, the software tool and the staff newsletter.

- ✓ The organisation has **information risk registers** and/or reports to enable relevant employees to record and manage information related risks (if any).

  Case study
  A council records data protection risks on corporate and operational risk registers, alongside its planned activities to mitigate those risks. The council also identifies risks as a result of information security incidents. Data protection steering group members discuss all risks, which are fed into the appropriate risk register. The registers are reviewed regularly and risks are escalated according to their likelihood and impact.

Records management

- ✓ The organisation makes **fair processing notices** readily available to inform data subjects how their personal data will be processed and (where applicable) shared.

  Case study
  A council's website privacy policy informs data subjects of their rights under the DPA and links to a more detailed page which clearly explains why the council collects personal data and what it does with it. Other pages contain details about how to access personal data and details of Information Sharing Agreements (ISAs).

  The council has also produced a social care booklet including guidance on what it does with personal data of this type, including access, security and sharing. The council call centre has a fair processing message that is automatically played to callers before their call is answered.

Requests for personal data

- ✓ **Key individuals and/or teams are responsible** for processing subject access requests.

  Case study
  A council's DPO is the corporate lead for subject access compliance. There are also local departmental leads and sub-leads for processing the actual requests. The DPO, local departmental leads and chair of the access to information steering subgroup are all members of the main data protection steering group. The subgroup meets regularly to approve subject access procedures, consider subject access compliance and provide a report to the steering group.

- ✓ The organisation performs **quality assurance** in regard to the redaction of information and the application of exemptions.

  Case study

A council DPO trains its social workers to do their own redactions. Managers across all directorates check any redacted information. The DPO also quality checks most responses, but may not have any further input if the request is simple. In response to subject access requests, the council explains any redactions or exemptions it has applied in its covering letters.

Security of personal data

✓ The organisation assigns **information security** responsibilities to establish relevant ownership and responsibility within the corporate information security framework.

Case study
The SIRO is the strategic lead for information security at the council. As the operational lead, the Information Security Manager maintains the corporate log of data security incidents. The data protection steering group, which approved the Information Security Policy and either closes data security incidents or escalates them to the SIRO, communicates its messages via information security champions in each directorate.

✓ The organisation does **penetration testing** and/or uses intrusion detection software.

Case study
A council conducts regular internal and external penetration testing of its network to minimise the risk of external threats. It uses a computer-aided vulnerability assessment tool to identify risks to the network (eg open ports or missing security patches). The council has recently completed firewall and penetration testing.

Training and awareness

✓ Key individuals and/or teams take clear **ownership of and responsibility** for data protection training.

Case study
The council's Data Protection Policy sets out the requirements and strategy for data protection related training. The SIRO has lead responsibility for the provision of the training. The data protection steering group, which is accountable to the CMB, oversees the provision of the training to all staff and develops, regularly reviews and signs off the rolling training programme.

The Learning and Development Team is responsible for the content and availability of the training. The council has dedicated training officers and champions, and managers are responsible for ensuring that all staff, permanent and temporary, complete the training, including refresher training.

- ✓ The organisation compiles **reports**, and communicates them, to help it oversee data protection and information governance training.

  Case study
  The Learning and Development Team records and reports statistics about completed data protection training to operational management and the data protection steering group.

Data sharing

- ✓ Data sharing agreements are **signed off** by senior management.

  Case study
  Either the Chief Executive, or the chair of the most relevant board, signs off the council's information sharing agreements. Employees responsible for signing ISAs on behalf of the council have role-based experience of data sharing and council practices.

- ✓ The organisation maintains **logs of data sharing agreements** to ensure that disclosures and any bulk sharing of information is tracked effectively.

  Case study
  With the input of local champions from each service, the data protection steering group has created a central record of all the council's ISAs. The council also uses the information to help create departmental Information Asset Registers (IARs).

Areas for improvement

Organisations in this sector could enhance overall controls within the scope areas covered in some instances by introducing, developing or maintaining the following:

Data protection governance

- An **information governance strategy** is endorsed by the Board to coordinate and drive compliance with legislative, regulatory and best practice information management requirements.

  Case study
  A council's management framework, which should ensure it can effectively oversee data protection compliance, is underdeveloped and not defined in an information governance or data protection strategy.

- An agreed format, styling and version control process for all **policies and procedures** as well as a defined process for review, ratification

and approval, to ensure that such guidelines are consistent and fit for purpose and continue to remain so.

Case study
Services and/or individuals are able to create policies themselves. The council does not oversee these policies, which do not require approval from senior management. These policies do not follow an approved format or version control process, have named owners or enforce at least an annual review.

- A **forum** to help operational staff in raising data protection issues for wider and/or corporate consideration.

Case study
A council has no forum to facilitate operational staff raising data protection issues. Employees tend to raise data protection issues with the DPO and/or Legal Services directly.

Records management

- A corporate **policy framework** which sets out the management direction and support for the records management function.

Case study
Although the council's Data Protection Policy contains elements of records management guidance around quality and retention, it has no overarching Records Management Policy to document its approach to records management, support the records management function and to provide a framework for supporting documents such as retention schedules and more process driven guidance.

- A **comprehensive IAR** which identifies and logs what manual and electronic records it holds, what they contain, in what format and what value they have for the data controller; and which is used to continually risk assess those assets to ensure that it controls the data and keeps it secure.

Case study
A council has failed to implement and standardise the use of IARs in line with the direction provided by The National Archives, to reconcile what personal data it holds, where it holds that data, which IAOs are ultimately responsible for that data and undertaking any associated risk management.

- The incorporation of records management within a formal training programme, which comprises **mandatory induction** and periodic refresher training for all employees with access to personal data.

Case study

A council has no corporate Records Management Policy and no formal data protection training programme incorporating records management.

Requests for personal data

- A **corporate log** which tracks the receipt and processing of subject access requests and is also used to provide reports against key performance indicators, such as compliance with responding to requests within the prescribed 40 calendar day period.

  Case study
  A council logs subject access requests on a central database which was primarily developed to record freedom of information requests and thereby, includes some fields which are not applicable to subject access and omits others which should capture key information such as the relevant day. Additional logging in the directorates has similarly been designed for freedom of information and may not capture subject access requests which are directly processed by operational employees instead of departmental leads. The council has no corporate nor localised reporting of subject access performance to help it monitor and address compliance concerns.

- A mandatory and monitored **training programme** for the key employees responsible for processing subject access and third party requests for personal data.

  Case study
  A council has not given formal specialised training to most employees processing subject access requests, and they tend to consult Legal Services for relevant advice.

- **Quality assurance** mechanisms in place to handle third party requests for personal data.

  Case study
  A council checks that third party requesters are authorised to request and receive the information. However, it does not carry out any subsequent monitoring or quality assurance checks on the disclosures.

Security of personal data

- Appropriate and mandatory **security awareness** training for all employees in the organisation and where relevant, contractors and third party users.

  Case study

A council has no mandatory foundation or regular refresher information security training for all employees and no advanced training for those employees in specialist information security roles.

Training and awareness

- Foundation and periodic data protection related **refresher training** in line with corporate and/or departmental requirements.

  Case study
  A council does not have a formal needs-based data protection training programme which applies to all staff and historically, data protection training has centred on the ad hoc delivery of basic presentations by the DPO at the request of team managers.

- Specific data protection **training for specialised roles** as appropriate, for example, a DPO, SIRO, Records Manager, IAOs and relevant employees responsible for subject access requests and data sharing.

  Case study
  A council provides specialised data protection training each year to departmental data protection leads, which focuses on areas such as changes in guidance and the application of exemptions. However, it has not provided significant specialised training to other key data protection roles such as the SIRO and the DPO.

Data sharing

- A formal **review process** to ensure that it removes or adds partner organisations to data sharing agreements as and when required, and to regularly examine the workings of the relevant agreements.

  Case study
  The responsibility for carrying out reviews lies with the directorate which owns the agreement as opposed to a key individual or relevant steering group. There is no corporate oversight to ensure that reviews are carried out on at least an annual basis.

Audit feedback and comments

Feedback is important as it helps us to improve. After we complete our audits we write to each organisation to ask for feedback on the audit process and tell us about their experience of the audit.

From the surveys returned for the period, we received the following comments:

- ✓ "The audit has given us the opportunity to improve and implement a much **better practice**."

- ✓ "The focus has **expedited data protection compliance** across many levels and highlighted the importance of good practices for the council. A very rewarding process."

- ✓ "It's **raised awareness** of staff, and expectations of senior officers. It has provided a **renewed focus** for information governance work and given it a greater priority. Overall I found all of the ICO staff I dealt with during the audit process helpful, friendly and knowledgeable. The process itself ran very smoothly and effectively, and I was able to clarify and confirm any issues I had, with ICO staff. As such I cannot think of anything that would improve an already **well organised** audit process."

- ✓ "It **improved the profile** of data protection compliance, which is welcomed."

- ✓ "The actions proposed in response to the report have yet to take effect but we anticipate that **data protection governance and practice** within the organisation **will improve**."