ICO Operations Directorate
Service guide

How we use public concerns, self-reported incidents and complaints to improve information rights practice

Contents

    - When the case is referred to another team
    - When the case is closed
- The 'prepare' work item

6. Progressing requests for advice

- Case types

7. Progressing DPA cases

- DPA concerns
    - Opportunity assessment framework
        - Is the ICO the right body to consider the matter?
            - Organisation not based in UK
            - If we do not cover the subject matter
        - Undue delay
        - If the customer has not raised the matter with the organisation responsible
        - Severity
        - The organisation's engagement
        - Other weighting matters
    - Explaining our decisions
    - Registration check
- Self-reported incidents
- Requests under s159 of the Consumer Credit Act
    - Initial checks
    - Dealing with some CCA s159 cases under the DPA
    - The process
        - Drafting a CCA s159 report
        - Drafting a notice, order and enclosing letters
            - 'No notice' orders
            - Orders with notices
- If the signatory disagrees with the recommendation
- **Concerns about CCTV operated by householders**
    - Addressing the issue with the customer
    - Addressing the issue with the CCTV operator
    - Concluding cases

8. Progressing FOIA/EIR cases

- What we expect from customers
    - To raise their concerns in good time
    - To provide the relevant documents
- What we expect from PAs
    - To revisit the request with a view to resolving the matter informally
    - To provide the information we need to make a decision
- Our investigation
- The decision notice

9. Progressing PECR cases

- Concerns about marketing text messages (SMS)
- Concerns about marketing phone calls – live
- Concerns about marketing phone calls – automated
- Concerns about marketing emails
- Concerns about marketing faxes

10. Taking action

- Options available
- Tasking and coordinating
- Keeping a record of ongoing action
- Monitoring the effectiveness of tasking and coordinating
- International cooperation

11. Closing, re-opening and creating new cases

- Closing cases
    - Closing DPA subject access delay cases
- RFA outcomes
- ELE outcomes
- FS50/EIR outcomes
- COM outcomes
- ENF outcomes
- Additional outcomes
- Description of outcomes
- Actions providing closure states for multiple cases
- Retention periods and rules for marking for preservation
- Re-opening cases
- Creating new cases

12. Managing communications

- Welsh language scheme
- Outgoing communications
    - Telephone
    - Email
    - Fax
- Incoming communications
    - Voicemail
    - Homeworking
    - Calls to the helpline
- Callbacks on cases
    - Callbacks on assigned cases
    - Callbacks on unassigned cases
    - No further contact (NFC) on cases

- Requests for prioritisation

- Signing off written communications
    - Information request paragraphs
    - Sign-offs
    - Prisoner communications

- Avoiding inappropriate disclosures
- Documenting communications
- Noting changes to contact details
    - Individuals
    - Organisations
- Dealing with follow up correspondence
- Staff welfare

13. Support for progressing cases

- Explanatory paragraphs
- Keeping it clear guide
- Policy advice and legal advice
- Information notices
- Special information notices
- Third party information notices
- Information with protective markings
- Cases with media interest (non-DN cases)

14. Feedback about our service

- Complaints directly from a party
    - Timescales
    - Disagreeing with FOIA decisions
- Complaints made through the PHSO

15. Other casework-related matters

- Cases about the ICO
    - Concerns about information requests – setting up the case
    - Concerns about information requests – progressing the case
    - Concerns about other DPA matters
- ICO employee cases
    - ICO staff submitting casework in their own name
    - If ICO employees are aware of someone they know submitting casework to the ICO
    - Staff who handle cases submitted by ICO employees
    - Publishing our casework performance
    - Concerns about keeping to this procedure
    - Duty of confidentiality
- Whistle-blowers
- Information requests for case-related information

Appendix 1 – Terminology

Appendix 2 – Related policies, procedures and resources

Appendix 3 – Service standards and relevant timescales

1. Overview

The ICO is the UK's independent public authority set up to uphold information rights. One of the ways we do this is by providing a range of services to the public. We advise individuals about their rights and obligations under information rights legislation. We also use our customers' concerns to improve information rights practice.

We can't look into every concern we receive and the law doesn't say we must. We will put most of our effort into dealing with matters we think give us the best chance of making the biggest difference to information rights practice.

Good information rights practice is not just about complying with the law. It includes the way organisations engage with the public and how clearly they explain their practices to them. Therefore, we will not usually look into a concern unless the individual has raised it with the organisation responsible. In turn, the organisation should engage positively with the individual, work with them to try to resolve their concern and explain their decisions appropriately. We provide tools and guidance to help with this process.

When someone raises a matter they have been unable to resolve with the organisation concerned, we will decide if we think there is an opportunity to improve information rights practice in that case or to address a more systemic concern. We will make this decision in light of the nature of the concern, our understanding of what has happened, the guidance we have produced and our experience of the relevant organisation or industry, among other things.

There are different forms of action we might take. We may simply offer advice to one or both parties. We may make a formal decision under the legislation we deal with, or ask an organisation to commit to an action plan, undertaking or advisory visit. Or we may consider more formal regulatory action.

In any event, we will be open about our work and publish information on our website about the concerns we have received, the actions organisations commit to and the regulatory action we take.

This guide gives information about our casework processes, but must be used alongside a large number of related policies and procedures. It will be reviewed periodically under the direction of the Operations Directorate.

2. Self-service

We will not look into an information rights concern unless the individual has raised it with the organisation responsible. In turn, we expect the organisation to work with the individual to try to resolve the matter. We provide tools and guidance to help with this 'self-service' process.

Tools for individuals

As well as providing advice on our website and through our helpline, we have produced some tools to help individuals deal with their concerns.

- 'Raising a concern with an organisation' – explains our general approach and that individuals should first raise their concern with the organisation responsible. It also gives an outline letter and general tips for raising concerns effectively.

- 'Concerns assistant' – a website tool designed to help people resolve their concerns with organisations and let them know when they have progressed their concern far enough to contact us. It also directs them to the right form for reporting their concern to us.

Tools for organisations

As well as providing advice on our website and through our helpline, and opportunities for meetings and audits, we have produced the following to help organisations.

- 'Information rights concerns – guidance for organisations' – explains our general approach. It says that individuals should first raise their concern with the organisation responsible, that we expect organisations to work with them to try to resolve it, what we will do if the organisation is unable or unwilling to deal with the concern and what we take into account when deciding whether to look into a particular matter.

3. Initial processes

The first stage of our casework process aims to get apparently eligible cases onto our systems and assigned to the right team.

Receipt and acknowledgement – paper correspondence

The Scanning Team receives and sorts most of the post for the Operations Directorate.

- **New cases**

New cases are scanned and acknowledged within one working day of receipt.

The written acknowledgement does not give a case reference number or say who will deal with it. However, it does tell the customer that we have received their correspondence and how quickly we expect to deal with it (whether it is a new concern, an enquiry, an information request, relates to an existing case or is copied correspondence). It also signposts additional information about our services.

- **Existing cases**

Correspondence that is obviously about existing cases is scanned directly to those cases. It is not acknowledged at this stage.

The Scanning Team provides regular scanning performance updates internally.

Receipt and acknowledgement – email correspondence

The Advice Service is responsible for managing our casework email inboxes in accordance with our inbox procedure (see **sift manual**, appendix 7).

All emails sent to these inboxes are automatically acknowledged on receipt. The email acknowledgement does not give a case reference number or say who will deal with it. However, it does tell the customer that we have received their correspondence and how quickly we expect to deal with it (whether it is a new concern, an enquiry, an information request, relates to an existing case or is copied correspondence). It also signposts additional information about our services.

- **New cases**

Rather than send everything to CMEH (as with the paper correspondence we receive), the Advice Service will delete, electronically file or respond to certain matters (such as obviously misdirected correspondence) before they reach CMEH.

- **Existing cases**

When a customer puts a correctly formatted reference number in the 'subject' header of their email, it will be forwarded to the right CMEH case automatically.

A correctly formatted reference has the following text in the subject field including the square brackets:
[Ref. XXXXXXXXXX] where 'X' is the case reference number.

If the email lacks a correctly formatted reference number, the Advice Service will attach it to the right case.

The sift

This is the part of the process where all the work received is sorted and passed to the group or team who will deal with it. The Advice Service will complete the casework sift in line with the Sift manual, dealing with some additional matters before classifying the remaining items.

This also includes recognising any cases which fall within the scope of the Independent Inquiry Into Child Sexual Abuse (the Goddard inquiry - for which there is currently no cut off point) and sending any (potentially) relevant case reference numbers to Information Governance, copying the email to the case so the case officer who picks it up is aware that Information Governance has been notified.

Relevant cases are cases which contain or may contain content pertinent directly or indirectly to the sexual abuse of children or to child protection and care. The following examples are by no means exhaustive but might help case officers identify them:

- Individuals who have, or may have been affected by these issues, have tried to obtain their personal data via a subject access request and have issues with that process or the results.
- Offenders or alleged offenders who may have tried to obtain any personal data about them via a subject access request.
- Self- reported security incident cases (or cases brought to our attention in other ways) where the subject matter of the information relates to the sexual abuse of children.

- FOIA complaints about information related to high profile cases.

FOIA appeals related to high profile cases.

Recording correspondence in Welsh

We report annually on the number of Welsh language enquiries (written and telephone) we receive and want a full understanding of the demand for our services in Welsh. To help us count the number of enquiries and complaints we receive in Welsh, we should add 'Welsh language' into the case title of any Welsh language case we sift.

Classifying cases

For work to be progressed in CMEH it must be classified. This means giving it one of the following case types:

INF – Misc. correspondence not requiring action but worth retaining
ENQ – Requests for written advice
IRQ – Formal requests for information held by the ICO
RFA – DPA concerns
ELE – PECR concerns
FS50 – FOIA concerns
FER – EIR concerns
COM – Self-reported incidents reported by a DC (but not whistle-blowers)
ENF – Formal regulatory action taken by the ICO
SEC – Request made under s159 of the Consumer Credit Act
PCB – Action taken when a potential criminal breach has been identified

The Advice Service will set the relevant case type as above, with two exceptions:

- A concern about the EIR will initially be set up as an FS50 case. After its allocation, the case officer will change the case type to FER.

- A request under s159 of the Consumer Credit Act will initially be set up as an RFA case. After its allocation, the case officer will change the case type to SEC.

If, when an officer fully considers a case, they decide that the original case type needs to be changed, they can do this as long as the case has not previously been closed. If it has, they should contact Operations Service Delivery.

Triaging self-reported incidents (from September 2014)

From September 2014, all self-reported incidents will be put in a dedicated work queue (work queue 3). They will be given the COM case type and be set as 'high' priority.

Staff in the Enforcement Department will triage this work each day to identify the highest risk self-reported incidents (the cases with the clearest potential to lead to a civil monetary penalty (CMP)). When they identify a high-risk case, they will assign it to an Enforcement work queue and add any relevant parties or attributes before progressing it.

They will set the priority of the remaining self-reported incidents to 'medium' and leave them in the Advice Service work queue. The Advice Service will then assign these cases to the appropriate sector group.

Potential criminal breaches

Matters which appear to constitute potential criminal breaches will be classified as requests for advice or concerns as appropriate (with the ENQ, RFA or FS50 case type) and assigned to the relevant sector group.

The Advice Service will also create a 'provide advice' work item and send it to the 'DP - RAD Investigations (Any)' queue to alert them to the potential criminal breach.

Staff in the Enforcement Department (Criminal Investigation Team) will aim to check each request for advice within three working days to identify the matters they can take forward as potential criminal breaches.

- **Cases progressed by Enforcement**

When Enforcement Department (Criminal Investigation Team) identifies a case they can progress, they will:

- create a new PCB case,
- copy across the relevant documents,
- assign the case to an Enforcement work queue, and
- add any relevant parties or attributes before progressing it.

They will complete the 'provide advice' work item and respond advising as such.

The original request for advice or concern case will remain in the sector team queue. Once allocated, the case officer should check the advice provided by Enforcement, to see if there are any additional matters to be dealt with. If there are, they should contact the relevant member of

Enforcement (the investigating officer if the matter is assigned, a manager if not) to ensure we take a coordinated approach where necessary.

If there are no additional matters to deal with, the case officer can close the case as 'Duplicate – marked for deletion'.

If there additional matters to progress, the case officer should deal with them in accordance with the relevant process.

- **Cases not progressed by Enforcement**

Where the Enforcement (Criminal Investigation Team) don't consider they can progress the case they will complete the provide advice work item, giving reasons why.

The case officer should then deal with the matter in accordance with the relevant process.

Sending cases to the sector groups

Using the following criteria, the Advice Service will assign:

- all concerns to the sector teams, and
- all enquiries not dealt with immediately to their own Advice Service work queues.

Work queue 1,2 & 4 Written advice that can't be dealt with immediately

Work queue 3 Self-reported incidents (from June 2014)

Work queue 5 All cases for work queues 6, 7 and 8

Work queue 6 PECR, RFA DPA telecoms, direct marketing concerns

Work queue 7 RFA DPA lenders and CRA concerns

Work queue 8 RFA DPA general business (including motor industry) concerns

Work queue 9 RFA DPA central government and finance (excluding lenders) concerns

Work queue 10 RFA DPA police and criminal justice, MoJ, Home Office

Work queue 11 RFA DPA London boroughs, education, leisure, environment, charities concerns

Work queue 12 RFA DPA regulators, BBC, transport, health concerns

Work queue 13 RFA DPA local government

Work queue 14 FS50 FOIA central government concerns

Work queue 15 FS50 FOIA police and criminal justice, MoJ, Home Office concerns

Work queue 16 FS50 FOIA London boroughs, education, leisure, environment charities concerns

Work queue 17 FS50 FOIA regulators, BBC, transport, health concerns

Work queue 18 FS50 FOIA local government concerns

All cases – except for self-reported incidents – should be assigned to the relevant queue no later than three working days after being created in CMEH.

From June 2014 self-reported incidents should be assigned no later than five working days after being created in CMEH, to allow for the Enforcement check.

4. Allocating cases

New cases sent to sector-team work queues must be allocated to individual team members, who should promptly prepare and progress the case.

At this point, we have told the customer only that we have received their correspondence. We have not told them their case reference number or who will be dealing with it. The case must be allocated to a case officer quickly, so that we make our first, and perhaps only, contact with the customer in line with our stated service level.

We inform customers who send us their concerns that we will respond to them within 30 calendar days. To achieve this service level we must deal with most of the concerns we receive more quickly than this. Our internal service level is 14 calendar days from the date the case was added to CMEH. This means each team will have about 10 calendar days to allocate, prepare and progress the work from the date it reaches their work queue.

We need to meet this service level in as many cases as possible. So, in the unlikely event that a case goes to the wrong team, that team needs to identify and redirect it in good time for the right team to respond in accordance with the service level.

In simple terms, we need most cases to be underway within 14 days, but all must certainly be underway within 30 days.

It is for each team to decide how to allocate work. Some managers may briefly look at each case before allocating it, or they may ask someone to do this for them. Some may ask each officer to take a number of new cases each day or week. Others may adopt a combination of the two methods, depending on the experience of their team members. In any event, the Group Manager of each sector team must ensure that:

- all cases assigned to their work queues are with officers in good time for them to contact customers within the required service level, and

- they have a sufficient understanding of the cases their team is working on to be able to support their effective progression and closure.

Case officers must divide their time between starting enough new cases to enable us to meet our service level and focusing on closing ongoing cases within six months of them being created on CMEH (except for CMPs). They will need to adopt an approach that sees work progressed as soon as possible at all times.

5. Preparing cases

All unallocated cases have a 'prepare case' work item. The first task for each officer is to 'prepare' the case. This means:

- checking for potential criminal breaches,
- adding the parties they intend to deal with,
- checking for similar, ongoing cases,
- retrieving any documents the individual says they want us to return,
- managing any physical evidence, and
- managing any withheld, protectively marked information.

Checking for potential criminal breaches

Although matters which appear to constitute potential criminal breaches will be classified as requests for advice or concerns and assigned to the relevant sector group, a corresponding 'provide advice' work item will also be sent to the 'DP - RAD Investigations (Any)' queue to alert them to the potential criminal breach.

Staff in the Enforcement Department (Criminal Investigation Team) will aim to check each request for advice within three working days to identify the matters they can take forward as potential criminal breaches.

If a case officer is allocated a potential criminal breach before Enforcement has determined whether or not they can take the matter forward, they should not begin work on the case and alert their manager to the delay. The manager will then decide whether to contact Enforcement about the matter.

Adding parties

Officers should add the party information to their own cases, in line with the relevant part of the 'party manual' section of the CMEH user guide, being sure not to duplicate records that already exist.

It is also important to check the spreadsheets in the 'party contacts' table on the 'organisations of interest' ICON page, to check for preferred party reference numbers, aliases and specific contact information. Duplication of party records will adversely affect our ability to extract meaningful management information about that organisation.

If the case officer comes across what looks like a duplicate party record, they should check that the records do in fact relate to the same individual or organisation. If so, they should identify a 'main' record and attach all relevant contact points, contact information and all related cases to that record. They should also break the links between the cases and the

unwanted records, before finally changing the party 'status' from 'current' to 'marked for deletion'. The 'removing duplicate party records' process may be helpful here.

Group Managers should also arrange to add details of organisations their team contacts most often to the party record spreadsheet and keep this accurate and up to date.

We do not have general rules about how we should contact customers. But there will be cases when we make special arrangements at the individual's request or for our own purposes.

- **Service adjustments**

In addition to our legal obligations under the Equality Act, we want to be able to meet the individual needs of all our customers by making appropriate and reasonable adjustments to allow equality of access to our services and provide good customer service.

If a party already exists on our system, the case officer should check whether the reasonable adjustment check box is ticked. If so, they should consult any related records on the 'restricted contact' and 'single point of contact' databases to see what we have previously agreed.

If an individual does not yet exist on our system but their correspondence or the case suggests they need some help when dealing with us, and what they have suggested is reasonable in the circumstances, then the case officer should take the steps detailed in the 'ICO service adjustment operating procedure: customers'. This includes:

- making a record on the 'reasonable adjustments' database,
- notifying the Head of Customer Contact, and
- ticking the 'reasonable adjustment' check box on the CMEH party record.

- **Restricted contact**

Occasionally, some customers behave in a way we think is unacceptable or find difficult to deal with. In some circumstances, we may restrict how they access our service.

If a party already exists on our system, the case officer should check whether the 'restricted contact' box is checked and, if so, consult the related record on the 'restricted contact' and 'single point of contact' databases, to see what arrangements have previously been made. For further information, please see our Managing customer contact operating procedure.

Checking for similar, ongoing cases

It is important that case officers check for similar ongoing cases, as it may be quicker for an officer who is already familiar with the issues to deal with the matter. However, it is up to the relevant manager to decide how best to use their officers' knowledge and experience. Where there are similar ongoing cases the officer must bear this in mind when considering the opportunities assessment framework.

High Profile cases

Some cases involve high profile issues that have already or are likely to generate substantial scrutiny of the outcome. We need to deal with such cases effectively and in a manner that minimises any reputational risk. Case officers should therefore, check whether the matter is one that is likely to fall within our 'high profile case procedure', and follow that procedure accordingly.

Cases of potential interest to the Independent Inquiry Into Child Sexual Abuse (Goddard inquiry)

In connection with the Independent Inquiry Into Child Sexual Abuse (the Goddard inquiry) government departments, agencies and public bodies have been instructed to retain any and all information they hold which contains or may contain content pertinent directly or indirectly to the sexual abuse of children or to child protection and care.

The Advice Service will check for any cases that may contain such information during the sift process and will send any (potentially) relevant case reference numbers to Information Governance.

Relevant cases are cases which contain or may contain content pertinent directly or indirectly to the sexual abuse of children or to child protection and care. The following examples are by no means exhaustive but might help case officers identify them:

- Individuals who have, or may have been affected by these issues, have tried to obtain their personal data via a subject access request and have issues with that process or the results.
- Offenders or alleged offenders who may have tried to obtain any personal data about them via a subject access request.

- Self- reported security incident cases (or cases brought to our attention in other ways) where the subject matter of the information relates to the sexual abuse of children.
- FOIA complaints about information related to high profile cases.
- FOIA appeals related to high profile cases.

However, in the event that it is not apparent that a case may contain such information at the sift stage, it is important that any case officer asked to deal with any such case notifies Information Governance as soon as it does become apparent that the case may be relevant to the inquiry.

Retrieving documents

In some cases, a case officer will need access to the customer's original documents because the customer has asked for their return or they have not been scanned successfully to CMEH.

As we only keep original documents for six months, it is important that case officers respond to such requests sooner rather than later.

- **When a customer asks us to return documents at the outset**

If the customer has asked us to return their documents at the time of their submission, the Scanning Team will usually scan an '*original documents to be returned*' coversheet to the case, indicating this fact.

As the case officer is responsible for returning the documents, they should collect them from the Scanning Team. Unless they are planning to return them immediately, they should consider whether to log the information on the information asset register (see 'Managing physical evidence' section below[add link]).

Items containing sensitive personal data or financial data that the officer thinks could cause detriment if lost in the post should be returned by recorded delivery. All other items can be returned by standard mail. If in doubt, the officer should check how the customer sent the information to us and, where possible, send it back the same way.

When returning documents the officer should always refer to our 'ICO operating policy – avoiding inappropriate disclosures.'

When the officer returns the documents, they should add a note to the CMEH case saying:

'*Documents date stamped XXXX, returned to customer by standard post/recorded delivery no XXXX today*' (deleting as necessary).

- **When a customer asks us to return documents later**

If the customer contacts us later to ask us to return their documents, or if they made their request earlier but it was not immediately apparent, then the '*original documents to be returned*' coversheet will not have been scanned.

In these cases, the case officer should follow the document retrieval process on ICON before following the 'If the customer asks us to return documents at the outset' process above.

- **When a document has not been successfully scanned**

If a document has not been successfully scanned to CMEH, the case officer should again follow the document retrieval process on ICON.

Managing physical evidence

The Scanning Team scans most of the casework material we receive to CMEH. However, items such as discs, DVDs and large lever-arch files of cross-referenced documents can't or won't be scanned. Such items are known as 'physical evidence'. If a case has associated physical evidence, the Scanning Team will scan a coversheet to the file.

As soon as a case officer is assigned a case that has related physical evidence, they become responsible for that evidence. So they should immediately:

- collect it from the Scanning Team (who will retain a record of it),
- put a note on the 'notes' section of the CMEH case to say what they collected and when,
- log it on the information asset register, and
- store it safely within the area chosen by a sector team manager.

- **Referring the case to another team**

If at any point a case officer refers the case to another team, they must pass the physical evidence to them and,

- add a related note to the 'notes' section of the CMEH case, and

- update the information asset register to show its new location and the date it was transferred. This applies even to temporary, short-term transfers.

Case officers receiving such information – even on a temporary basis – should immediately check the information asset register to make sure it is accurate and up to date.

If a case officer transfers any physical evidence into the custody of someone else (for example the IS department if information needs to be extracted electronically), they should again update the information asset register accordingly.

- **When the case is closed**

We want to return physical evidence as soon as possible after a case is closed but we may need to consult it again if either party to the case contacts us again. The case officer must therefore use their judgement to decide when to return physical evidence, discussing it with their manager as appropriate.

When deciding to return physical evidence, the case officer must also consider the best way to return it. The primary consideration should always be the sensitivity of the data. There are some additional questions to consider when returning information to organisations in the 'returning information to third parties' section of the Security Manual.

However a case officer returns physical evidence, they should always:

- put a related note on the 'notes' section of the CMEH case, and
- update the information asset register saying when the records were returned and recording any tracking reference number that applies.

The 'prepare' work item

Separate processes follow for progressing the different types of cases we deal with at the ICO. However, in all cases, having considered the matters raised and contacted the relevant party or parties, the case officer must immediately complete the 'prepare' work item and create a new 'progress' work item in line with the 'work item manual' in the CMEH user guide.

Contacting the customer before completing the 'prepare' work item allows us to use the completion of this work item to measure performance against our 14-day service level.

6. Progressing requests for advice

Our Advice Service is responsible for dealing with most requests for advice in writing. Where requests are about new or novel issues, the Advice Service will work with colleagues from across the office to develop responses. Requests for advice may also be referred to colleagues outside the Advice Service where it makes sense for them to own the contact with the customer. However, we only expect this to happen in a few cases.

The Advice Service responds to most requests for advice at the same time as it sifts through all the work received by the Operations Directorate. This means most customers receive their response very quickly, usually only a few days after we received their enquiry.

Requests that we can't respond to immediately, usually because some research is needed, are allocated to the Advice Service work queues. In most cases, an officer will deal with these requests within 14 calendar days. We aim for all requests to be dealt with within 30 calendar days.

Wherever possible, the Advice Service will try to contact customers by phone. We encourage customers to give us a day-time phone number.

- **Case types**

All requests for written advice are dealt with under the ENQ case type, whatever information rights legislation they relate to.

If a customer has a concern or complaint about a named organisation, but the matters clearly fall outside our jurisdiction, the Advice Service would respond using the case type appropriate to the legislation involved, add the customer's name and the name of the organisation they are concerned about to the case, and select the appropriate case outcome. We take this approach so that we can retrieve this work when we are analysing the concerns we have received about a particular organisation or sector.

7. Progressing DPA cases

Once they have 'prepared' the case, the case officer should begin to consider it.

A DPA-related case will usually be:

- a DPA concern,
- a self-reported incident, or
- a request under s159 of the Consumer Credit Act.

DPA concerns

Individuals may raise DPA concerns about the way their personal data has been processed and how organisations have handled their information rights complaint. As regulator, we have to consider how organisations are complying with their obligations under the law. We want to ensure that we use information shared with us to improve information rights practice where this is appropriate.

Under s42 of the DPA, individuals who are directly affected by the processing of personal data (or their representative) can ask us to assess the likelihood that the processing of their personal data complied with the DPA. It is then for us to tell them what – if any – action we, as the regulator, intend to take.

We have considerable discretion when considering compliance with the legislation. For example, we can choose to reach our decisions based solely on the information provided by the customer raising the concern, if we consider it appropriate. However, we will always tell an organisation if we think they have breached the DPA.

We will put more resource into reaching decisions if the matter appears to enable us to improve information rights practice.

Case officers should consider their decisions about what we intend to do in the context of the opportunity assessment framework.

Opportunity assessment framework

The opportunity assessment framework (OAF) is a series of matters that case officers should consider to help them initially assess the severity of a concern and consider the opportunity it may give us to improve information rights practice.

It is not an exhaustive list of questions to be answered in a particular order and it doesn't say what action officers should take. It is simply a series of things all officers should think about to help ensure we're approaching cases consistently. Case officers do not need to make a record of their thinking, as the key points will likely be recorded in any related letter or letters they send.

The guidance below will help in some of the areas for consideration. It does not cover all the matters to be considered, many of which are self-explanatory.

- **Is the ICO the right body to consider the matter?**

The case officer will not normally need to consider the OAF in a particular order, but should usually first decide whether the ICO is the right body to consider the matter.

The ICO obviously won't be the right body to consider a matter when it doesn't concern the legislation we are responsible for. However, sometimes the concern will relate to matters that intersect with another organisation's responsibilities and we have previously agreed they will deal with such matters, perhaps in an MoU. For more information, see the 'working with other bodies' section of our website.

The Advice Service will identify and deal with the concerns that we most obviously shouldn't deal with. However, sometimes it may only be possible to know this with the benefit of sectoral knowledge or having conducted some investigation first.

Although this is not an exhaustive list, the cases we're most likely to be able to identify as falling outside our remit at this stage are those where:

- the organisation responsible is not based in the UK, or
- the subject matter is not something we cover.

If a DPA case relates to an organisation based in the EEA (except the UK) and the document needs translating, the case officer should contact Corporate Affairs to arrange for translation.

If and when we get an English version, the case officer should decide whether or not the data in question is being processed in the UK.

- If it is, they should deal with it as normal (see below).

- If it isn't, they should let the customer know the matter is outside our jurisdiction and provide the address of the European data protection authority that can help.

- If it isn't clear, ask Policy Delivery for help.

If the matter relates to an organisation based outside the EA, we should let the customer know we cannot help.

- **If we do not cover the subject matter**

If the subject matter is not relevant or we have previously agreed it should be dealt with elsewhere, the officer should let the individual know.

If we are aware of an organisation that is better placed to help, even when there is no formal agreement between us, we should give relevant details to the individual. See the helpline directory for the details of the organisations we most commonly refer customers to.

- **Undue delay**

The case officer should also consider whether the customer has delayed raising the matter with us. In this case, a 'delay' is three months or more.

This is not a strict cut-off. But if a customer raises a concern with us more than three months after their last meaningful contact with the organisation responsible, we would not expect to investigate the concern unless there appears to be an obvious opportunity to improve information rights practice. Instead, we would likely base our response on the information provided by the customer.

- **If the customer has not raised the matter with the organisation responsible**

The OAF asks the officer to consider whether the customer has raised the matter clearly with the organisation responsible. Unless it would be unreasonable or inappropriate for them to do so (for example, as might be the case with whistle-blowers, or when the matter appears to be serious or affect a large number of people), we should tell them to do so, referring to the tools we provide to help them. The officer should then close the case, selecting the relevant outcome.

- **Severity**

The OAF also asks the officer to consider whether the matter is serious, in terms of the nature of the data affected, the number of people affected, and the effect (or likely effect) on the individual(s) concerned.

The more serious the breach, the more likely it is we will take action in relation to a matter. Seriousness is a measure of how significant the data controller's failure to comply with the DPA is. For example, the failure to encrypt portable media containing sensitive personal data would be considered a serious incident if such a device was lost or stolen. The nature of the data compromised is also relevant. A case concerning sensitive data or data which is otherwise likely to have a significant impact upon the affected data subjects is more likely to conclude by way of formal regulatory action. The number of data subjects affected can also be a factor. However, it does not follow that action will always be appropriate in these cases, and it does not mean that we won't take action where the matter does not appear to be 'severe' in those terms.

- **The organisation's engagement**

The OAF also asks the officer to consider how the organisation responsible has dealt with any concern raised by the individual about this matter. The case officer should consider how well the organisation engaged with the customer, whether and how well it explained what had happened and whether it made reasonable attempts to rectify any problems.

If the customer has raised the matter with the organisation responsible and it has not responded properly, then, if is not unreasonable or inappropriate to do so, the case officer should contact both parties, referring the organisation to the tools we provide to help them, and close the case, selecting the relevant outcome. When setting target response dates for new cases, case officers should aim to be transparent in explaining what is required from the organisation and explain why particular timescales have been set when entering into any correspondence.

- **Other weighting matters**

The OAF also asks the case officer to consider the concern in the context of any other relevant information we may hold about the matter, the organisation responsible or the relevant sector. The officer should therefore consult any information held by their team as well as by other departments (including the sector pages on ICON). The case officer may also raise the matter at a tasking and coordinating meeting with their manager's agreement.

Explaining our decisions

When the case officer has made their decision, they should tell the customer the outcome and whether or not the ICO intends to take any action.

We should provide clear reasoning behind any recommendations that we make to organisations. This is to provide assurance that the recommendations are proportional, add value and mitigate the issues arising.

When explaining our decisions the officer should use language appropriate to the situation. If, based on the information provided, the case officer is clear that the DPA does not prohibit the processing, the officer should say so clearly and definitively in response. If, however, things are not so clear, then terms like 'likely' or 'unlikely' may be appropriate.

In any event, the case officer should avoid saying (or implying) that the only purpose of our consideration is to decide how likely it is that an organisation has complied with the DPA. Instead, they should be clear that our consideration is to help us decide whether further action is merited to address a serious contravention of the law.

The officer should also let the individual know that if the customer thinks we should have done something differently in the way we handled their concerns, or otherwise treated them, they can let us know in line with the 'service standards and what to expect' section of our website.

Registration check

The case officer should also search the public register to establish whether the organisation has a current registration (but need not do so if we often contact it and are satisfied it is registered). If the organisation lacks registration and a clear exemption, the case officer should give it relevant information.

Self-reported incidents

Where organsiations experience a serious data security breach, we ask them to report it to us via our security breach notification form. The 'notification of data security breaches to the ICO' guidance sets out the circumstances in which reporting is considered appropriate. This includes incidents which have affected a large number of people; where particularly sensitive data has been placed at risk; and where data is at continued risk of inappropriate processing. The most serious incidents tend to concern the theft, loss or inappropriate disclosure of sensitive data.

In general, Enforcement staff deal with the most serious cases and the sector teams deal with the rest. Enforcement staff triage self-reported incidents daily to identify the highest-risk incidents and to assign them to their queue.

However, if a sector team looks at a matter that turns out to be more serious, it will continue to gather the necessary information to understand the incident fully. If formal regulatory action is then to be considered, the case would be referred to the relevant tasking and coordinating group. Although Enforcement would take the lead on any formal regulatory action case, the original case officer would remain involved.

Officers should consider what action to take in response to the self-reported incident. Some of the questions in the opportunity assessment framework are likely to be useful.

Requests under s159 of the Consumer Credit Act

Requests under s159 of the Consumer Credit Act (CCA) will initially be set up as RFA cases. After their allocation, the case officer will change the case type to SEC as long as the case has not previously been closed. If it has been closed, the case officer should contact a member of Operations Service Delivery for advice.

Under s159 of the CCA, if an individual considers an entry on their credit reference file is wrong and if it is not corrected they are likely to be prejudiced, they can ask the relevant credit reference agency (CRA) to remove or amend it. The CRA should respond within 28 days. If the CRA does not respond within 28 days or does not remove the entry, the individual can ask the CRA to add a Notice of Correction (a statement of up to 200 words, which an individual can have added to their file next to the entry they think is wrong).

If the CRA considers the notice is incorrect, defamatory, frivolous or scandalous, or is for any other reason unsuitable for publication, it will not add it to the file, but will refer it to the Information Commissioner. The Commissioner will then make an order to say what notice, if any, the CRA should add. Individuals can also apply directly to the Commissioner. In so doing, however, they may lose the opportunity to have their own wording including as any notice he orders will be his words, not the complainant's.

Orders made in connection with notices may only be signed by individuals specifically authorised to perform the Commissioner's functions under s159 of the CCA. However, case officers are responsible for initially dealing with CCA s159 cases and recommending the action we should take, in line with this procedure.

Initial checks

Most s159 cases are referred by CRAs. The case officer should check that the CRA has provided:

- a copy of the individual's credit reference file which shows the disputed entry or entries,

- a copy of the individual's notice, and

- an explanation as to why the CRA considers the notice unsuitable for publication.

If the CRA hasn't done these things, the case officer should ask the CRA to do so.

Dealing with some CCA s159 cases under the DPA

If it appears that the disputed entry is inaccurate or has been recorded unfairly, the case officer should deal with the matter in line with the casework process for DPA concerns.

This is because if the entry is removed or corrected as a result of that process, there will be no need to add a notice.

In these cases, the case officer should change the case type from SEC to RFA.

At the end of that process, relevant explanations as to why a notice is no longer necessary should be given to the relevant parties.

The process

The case officer should contact the CRA, the individual and the lender concerned, to explain that the matter has been referred to the ICO and to ask for representations, using the relevant CCA s159 example letters (initial letter to CRA, initial letter to individual and initial letter to lender) as a guide.

On receiving their responses (or when the response deadlines have expired) the case officer should decide whether a notice should be added.

There are several reasons why the case officer may decline a notice and recommend a 'no notice order'. The most common are as follows:

- **The lender indicates that the entry has been amended or deleted as a 'gesture of goodwill'** – where the amendment/deletion has been made and there is no indication that the entry contravenes the DPA.

- **A notice may adversely affect an individual's creditworthiness** – and it would not, therefore, be in the individual's interests for us to order that a notice be added to their file.

The point to remember here is that the Commissioner is under no duty to order a notice. It is entirely at his discretion.

- **Drafting a CCA s159 report**

Whether the case officer decides we should add a notice or not, they should draft a report, using the example CCA s159 - report as a guide. They must write this on the basis of the information available, even if we don't feel we have a full picture of the relevant circumstances.

- **Drafting a notice, order and enclosing letters**

If the case officer decides to add a notice, they will usually need to re-draft the notice written by the complainant, considering the following points.

- A notice will be linked to a specific entry or entries recorded on the individual's credit file.

- Although on a strict reading of s159 of the CCA 1974, a notice is intended to allow comment on a record the individual believes to be incorrect, the Commissioner has permitted notices of explanation and qualification. This is because, if the individual gives plausible grounds why a particular adverse account record could give a misleading impression of their creditworthiness, the record, though accurate, could be misleading.

- Draft the notice in the third person (ie, using 'The Commissioner' and 'he'), to make clear it is the Commissioner's notice.

- Write a balanced notice. If the individual makes assertions the lender disputes, make clear that the lender disagrees.

- Be concise. You only have 200 words so you should give a clear indication of the grounds on which the entry is disputed, while avoiding the minute detail of the dispute.

- Avoid using the word 'believe' when representing the views of the parties involved. We should not presume to know exactly what the individual thinks about the matter. Use 'maintains', 'says' or 'seems to believe' instead.

- Do not name any lender(s) involved in the dispute. When an organisation searches a file, it does not see the names of organisations that filed the account information. As naming specific lenders could encourage certain types of direct marketing, we will not usually name any lender in a notice.

Using the relevant templates, the case officer should then draft the following:

- an order (order – with notice, order – no notice),
- an enclosing letter to send to the individual (individual - order - notice to be added, individual - order - no notice), and
- an enclosing letter to send to the CRA (CRA - order - notice to be added, CRA - order - no notice (leaving the 'date of issue' of the order blank).

If the lender responded to the case officer's initial letter asking for a copy of the order, the case officer should also:

- write to the lender, using the relevant example letters as a guide (lender - order - notice to be added, lender - order - no notice).

The case officer should then send their recommendations to the designated order signatory (via a 'provide advice' work item) who may want to discuss them further.

- '**No notice orders**'

If the signatory agrees that no notice should be ordered, the relevant orders and letters should be sent and the case closed in line with CCA s159 section of the CMEH user guide.

- **Orders with notices**

If the signatory agrees we should order a notice, then the notice, orders and letters should be sent. The case officer should then monitor the case. This is to check that the CRA sends the copy of the amended credit reference file as requested.

Once the CRA has sent the amended credit reference file, and the case officer is happy it has fully complied with the order, they should close the case in accordance with the CCA s159 section of the CMEH user guide.

NOTE – where a notice has been ordered on a s159 case, the case officer should tick the 'review for preservation' box on CMEH when closing the case.

If the CRA does not send the amended credit file within the relevant timescale or the case officer is otherwise unhappy with its response, they should discuss the matter with the signatory.

If the signatory disagrees with the recommendation

If the signatory disagrees with the case officer's recommendation, they will discuss the matter with them. Ultimately, they may ask the case officer to draft a new notice, order and enclosing letters as appropriate.

Concerns about CCTV operated by householders

Where a customer is concerned about a surveillance system (such as CCTV) that is being operator by a private householder (such as a neighbour), our approach will be slightly different.

In some cases, customers may have good reasons why they can't approach a household CCTV operator. Even if they did approach the operator, it may be difficult for the customer to get evidence that the surveillance system is capturing personal data beyond the boundaries of the operator's property. For these reasons, we will not always expect the customer to exhaust the usual 'self-service' options before we will look into their concerns. Sometimes, this will mean accepting DPA concerns without any evidence that the CCTV system is actually subject to the DPA.

We will take an advisory approach to these cases, aiming to:

- help the customer understand what they can do to reach resolution with the CCTV operator (where appropriate), and/or either
- helping the CCTV operator understand what they can do to ensure their system is not subject to the DPA, or
- helping the CCTV operator understand what they should do to ensure their system complies with the DPA.

We have a legal duty to make an assessment (in many cases) and we aim to improve information rights practices. We should remember that in these cases in particular, improving the information rights practices of the CCTV operator may bring the biggest benefit to the customer.

Addressing the issue with the customer

Where possible, customers should first attempt to resolve the situation directly with the CCTV operator.

Where that is not possible, we should explain our aim to improve information rights practices by advising the operator about how they might operate their system so that it doesn't unnecessarily affect the privacy of others. We can advise on the steps that they can take so that their system complies with the DPA or otherwise is not caught by it (eg their system only captures footage within the boundaries of their own property).

Before contacting the CCTV operator about the customer's concern, we must ensure that the customer has clearly consented to us disclosing their identity to the CCTV operator. In some cases, the customer may wish to remain anonymous, even if this means it impossible for us to look into the matter.

Addressing the issue with the CCTV operator

It is important to remember that in many cases, CCTV operators will be unaware that they may be subject to the requirements of the DPA.

After explaining what the law requires, we should look for any reasonable opportunity to encourage the operator to attempt to resolve the customer's concerns with them directly, where this is appropriate.

We should also give guidance on how they might operate their system so that it doesn't unnecessarily affect the privacy of others, and so that it complies with the DPA or otherwise is not caught by it.

We should ask the operator to respond to us by a specified date. We should give multiple options - post, email and particularly a telephone number - to make this as easy as possible.

If we have trouble obtaining a response, as with all DPA cases, we should use our discretion to decide how to progress the matter, depending on the circumstances. We will take a proportionate approach in all cases. If a Case Officer is unsure how to proceed, they should ask an LCO or their manager.

If we are asking the CCTV operator to take specific action in response to a concern (for example, providing access to personal data held as CCTV footage, or providing a response to a notice made under section 10 of the DPA) Case Officers should again ask their LCO or manager for guidance.

Concluding cases

Where an informal resolution cannot be reached, and CCTV operators are unable to ensure that their system only captures footage within the boundaries of their own property, we will advise both parties of the rights individuals have in relation to CCTV systems caught by the DPA and the obligations on those operating such systems.

In some cases, we may close the case after explaining these rights and obligations. In other cases, we may take further action such as scheduling a tasking and coordinating meeting. However, as with all DPA cases, the way we progress them must be informed by the facts of the case and the relevant considerations outlined in the OAF.

8. Progressing FOIA and EIR cases

Under s50 of the FOIA, a person who is unhappy with the way a public authority has dealt with their information request and request for review can raise it with us.

Before we deal with an FOIA complaint, we expect PAs to have considered the issues around withholding the information in detail and shared them with the complainant during their internal review.

What we expect from customers

- **To raise their concerns in good time**

Under the FOIA we can refuse to consider complaints and concerns raised after an 'undue delay'. Our threshold is three months.

If customers raise FOIA complaints or concerns more than three months after their last meaningful contact with the public authority, we would usually expect to refuse to consider them unless extenuating circumstances apply.

- **To provide the relevant documents**

We usually expect to be provided with copies of:

- the FOIA request,
- the PA's response, including any refusal notice, and
- any internal review decision they have received.

What we expect from PAs

When we receive a valid complaint, we will give the PA one opportunity to justify its position before issuing a decision notice.

- **To revisit the request with a view to resolving the matter informally**

We prefer complaints to be resolved informally if possible. We therefore ask the PA to revisit the request and see if they can reverse or amend their position in light of our guidance.

If this results in them giving the information to the complainant, we may be able to close the case informally without the need for a decision notice.

- **To provide the information we need to make a decision**

In any event, if the matter cannot be resolved informally, the case officer should also ask for the information they need to make a decision. When setting target response dates for new cases, case officers should aim to be transparent in explaining what is required from organisations and explain why particular timescales have been set when entering into any correspondence.

During the review the PA may change – or add to – the exemption(s) they originally relied on. In these cases, the case officer should consider the new exemption(s).

Our investigation

After receiving the PA's response, the case officer will consider it.

Depending on the complaint, the case officer may consider:

- what searches the PA did to determine it did not hold the information,
- the exemptions the PA applied and whether it applied them correctly,
- the factors the PA considered in gauging the public interest in the information,
- what, if any, harm could occur if the information were released, and
- the PA's basis for refusing the request on the basis that it was not valid, was vexatious or was repeated.

The case officer should also take into account case law, legislative requirements and developing precedent, along with any other relevant guidance, with specific reference to the policy delivery knowledge base. Further resources are available at 'Standard (FOIA) casework guides, forms and letters'.

We should provide clear reasoning behind any recommendations that we make to PAs. This is to provide assurance that the recommendations are proportional, add value and mitigate the issues arising.

The decision notice

After concluding the investigation, the case officer will draft a decision notice for the Commissioner or another senior member of staff to approve.

The decision notice will set out the Commissioner's final decision in relation to the application under the FOIA or EIR.

The signatory will check that the decision notice has been adequately researched, reasoned, evidenced and drafted. Once a decision notice has been signed-off, the case officer should complete a number of administrative tasks, in line with the relevant 'signing off a case with a decision notice' process. The Commissioner cannot withdraw or amend a decision notice after issue.

9. Progressing PECR cases

Once they have 'prepared' the case, the case officer should begin to consider it.

Generally, the valid concerns reported to us under PECR involve marketing messages communicated by:

- text message,
- telephone – call from a live person,
- telephone – via an automated message,
- email, and
- fax.

We also receive requests for advice about the more technical provisions in the legislation.

Concerns about marketing text messages (SMS)

It is difficult for us to take action in relation to a single, unwanted marketing text message. We have therefore introduced a 'report your concerns' tool.

We ask customers to put details of the message they received into the tool. This allows us to collect data about repeat 'offenders', which will help us take action in the future.

When we receive an individual concern through another means, the case officer should:

- add details to the reporting tool,
- contact the individual to explain what we have done,
- close the case, and
- consider whether further action is appropriate.

Concerns about marketing phone calls – live person

It is also difficult for us to take action in relation to a single, unwanted marketing call. We therefore also ask customers to put details of the call they received into the 'report your concerns' tool, so we can collect data about repeat 'offenders', which will help us take action in the future.

When we receive an individual concern through another means, the case officer should:

- add details to the reporting tool,
- contact the individual to explain what we have done, and provide advice about stopping further calls,
- close the case, and
- consider whether further action is appropriate.

Concerns about marketing phone calls – automated

It is also difficult for us to take action in relation to single, unwanted automated calls. We therefore ask customers to put details of the automated call they received into the 'report your concerns' tool. This allows us to collect data about repeat 'offenders', which will help us take action in the future.

When we receive an individual concern through another means, the case officer should do the following:

- If the message advertises a premium rate number, advise the customer to complain to PhonepayPlus.
- If not, add details to the reporting tool.
- Contact the individual to explain what we have done.
- Close the case.
- Consider whether further action is appropriate.

Concerns about marketing emails

It is difficult for us to take action in relation to a single, unwanted marketing email message. We have therefore introduced a 'report your concerns' tool.

We ask customers to put details of the message they received into the tool, and attach the marketing email. This allows us to collect data about repeat 'offenders', which will help us take action in the future.

When we receive an individual concern through another means, the case officer should:

- add details to the reporting tool,
- contact the individual to explain what we have done,
- close the case, and
- consider whether further action is appropriate.

Concerns about marketing faxes

Customers can report their concerns about marketing faxes via our website.

On receiving a complaint about marketing faxes, the case officer should do the following:

- When possible, contact the sender to ask them to suppress the customer's details and for relevant details about their marketing practices.
- Contact the customer to explain what we have done and how to prevent further faxes.
- Close the case.
- Consider whether further action is appropriate.

10. Taking action

Options available

We can't look into every concern we receive and the law doesn't say we must. We will put most of our effort into dealing with matters we think give us the best chance of making the biggest difference to information rights practices ('priority cases'), either in the individual case, or to address a more systemic concern.

When considering a case, the case officer will take an initial view as to whether a matter is a priority case. They will form this view in light of the organisation's response to the individual, ICO guidance, what we know of the sector, industry and organisation concerned, and any other information they consider relevant.

If the case officer believes that a matter is a priority, they should consider what type of action would be most appropriate and effective in the circumstances. The potential options available include, but are not limited to, the following. (Note – where the suggested action relates to the work of another department, that department must first be consulted, in accordance with the processes detailed below.)

- Telling an organisation we have received a concern about them that we are keeping on file (e.g. where a matter has been corrected and there is no further action to take, but we want the organisation to know we know about it.)

- Asking an organisation to respond to a concern an individual has raised with them or giving advice about their response processes.

- Asking an organisation to put right what went wrong in a particular case (e.g. respond to an overdue SAR).

- Asking an organisation to contact individuals who may not know their personal information could have been compromised (e.g. the information has been subject to a security breach that has now been rectified).

- Contacting an organisation known to be responsible for sending marketing messages in potential breach of the DPA or PECR, asking them to confirm suppression of contact details and give information about their marketing processes.

- Exchanging information with the Telephone Preference Service about telemarketers with multiple PECR breaches.

- Asking an organisation to produce an improvement or action plan to make broader changes (e.g. to make improvements to policies and procedures that seem unfit for purpose).
  Encouraging an organisation to sign up to an information risk review or advisory visit from Good Practice.

- Encouraging an organisation to request a voluntary audit by Good Practice.

- Exerting influence over an organisation or industry through our Strategic Liaison contact.

- Exerting influence over an organisation or industry in partnership with another regulator, trade body or association (e.g. delivering key messages in industry press or industry workshops).

- Asking an organisation to sign up to a formal undertaking, in line with our undertakings guidance (currently being amended).

- Taking formal regulatory action in accordance with our Data protection regulatory action policy (e.g. by issuing an enforcement notice or a civil monetary penalty).

This is not an exhaustive list. Any action (or actions) we recommend must be tailored to the circumstances of the case. Case officers are encouraged to look for and suggest new and creative solutions to help organisations improve their information rights practices.

Tasking and coordinating

In some cases, it will be clear that action can be taken solely within the six sector groups and without affecting the ICO's broader work. However, it is likely that a small percentage of concerns will require coordinated action alongside others.

Whenever we consider the concern requires input from or action by another ICO department, has the potential to affect other operational activities, or may have a significant impact on information rights , we must ensure a suitable level of cross-office coordination. In those cases, officers should seek the views of other departments, through the 'tasking and coordinating' process.

Sector-based tasking and coordinating groups meet fortnightly to:

- share information about concerns,
- identify and discuss possible solutions,
- allocate and coordinate tasks to individuals or departments, and
- monitor and review the effectiveness of any action taken.

Having decided that a matter may be suitable for 'tasking and coordinating', the case officer will complete a proportionate amount of research into the nature and background of the concern, ICO guidance, current or historic behaviour of the organisation, links to other concerns or issues, and anything else they feel is relevant; and bring all this information to the meeting.

They should also provide an outline of the matter to the chair (usually a Group Manager involved in casework. The case officer should then complete the sector tasking and coordinating spreadsheet.

If a concern is urgent and cannot wait until the next scheduled meeting, the case officer should inform their manager with a view to asking the chair to hold an ad hoc tasking and coordinating meeting.

Issues of concern or sectoral interest may also be referred to the relevant tasking and coordinating group by other ICO departments, for example, Strategic Liaison, Enforcement or Good Practice. This will be done via the Intelligence Hub and by adding details to the spreadsheet .

Opportunities to address concerns or issues at a strategic level may be elevated to the ODDH, a wider pool of department heads and/or IRC to enable the ICO to set new priorities and strategies or launch proactive campaigns or initiatives aimed at addressing the issue.

The 'Tasking and coordinating groups - terms of reference' gives further information about the purpose, responsibilities and membership of the tasking and coordinating groups.

Keeping a record of ongoing action

Each chair will ensure that notes of sector-based tasking and coordinating meetings are taken. Actions and decisions should be recorded on the relevant sector tasking and coordinating spreadsheet in Meridio, so they can be accessed by other group members and the Intelligence Hub. When cases are closed, the case officer should select the most appropriate 'outcome' from the CMEH dropdown list, in light of the actions taken.

Monitoring the effectiveness of tasking and coordinating

The tasking and coordinating groups will review any action taken as a result of their discussions, with a view to measuring its effectiveness.

The Intelligence Hub will produce composite reports from the minutes of all the tasking and coordinating group meetings for ODDH. ODDH will raise relevant matters for discussion with IRC.

International cooperation

In cases where the data controller may be established in another jurisdiction, or in multiple jurisdictions it may be appropriate to consider international cooperation. This may also apply where the data controller is established in the UK, but affected data subjects are also in other countries.

A checklist and supporting guidance has been created to assist Officers in cases where international cooperation is being considered. In these cases the Intelligence Hub should be consulted in the first instance. It may also be appropriate to discuss these issues at a tasking and coordinating group meeting.

- International Enforcement Co-operation - Instructions for checklist
- International Enforcement Co-operation - Checklist

11. Closing, re-opening and creating new cases

Closing cases

When closing a case the officer is responsible for completing all outcome and attribute information.

When reporting on our work we want to be clear about how many cases required formal consideration and how many we closed after providing advice. For example, if an individual raises a concern under FOIA, we will consider it under the FS50 case type. If it turns out that the individual's concern fails to meet the threshold for formal consideration set out under FS50 of the FOIA, and the case officer informs the customer of this, then they should record the outcome as 'Closed – not s50', or 'Closed – not PA' etc, rather than change it to an ENQ and close it as 'advice provided'.

The Operations Service Delivery Group will provide regular 'exception reports' identifying cases with incomplete closure information. Officers will be expected to minimise their appearance on this report and take immediate steps to correct any entries. All managers are responsible for ensuring the information their teams enter onto CMEH is of a sufficiently high quality.

The outcomes for each case type are listed below, along with explanations as to when a case officer should use them.

Closing DPA subject access delay cases

When closing a DPA case that was primarily concerned with a delayed subject access request, the Case Officer should make sure that both the 'Nature 1' and the 'Nature 2' fields on CMEH are recorded as 'Subject access'. The Case Officer does not have to wait until closing the case before selecting these fields, but you should conduct a final check at closure to make sure you have done so. To be clear this dual recording of 'Subject access' applies to subject access cases that are concerned with delay only.

RFA outcomes

- DC outside UK
- Not DPA
- Concern to be raised with DC
- Response needed from DC
- No action for DC
- General advice given to DC
- Compliance advice given to DC
- DC action required
- Improvement action plan agreed
- Undertaking served
- Advisory visit recommended
- Compliance audit recommended
- Enforcement notice pursued
- Civil monetary penalty pursued
- Criminal investigation pursued

ELE outcomes

- Insufficient information provided
- PECR does not apply
- Insufficient evidence of breach
- Enforcement not recommended
- Enforcement pursued

FS50/FER outcomes

- Insufficient evidence
- Not PA
- Not s50
- Not EIR
- Vexatious
- Frivolous
- No internal review
- Undue delay
- Abandoned

- Withdrawn informally resolved.
- Decision notice served – not upheld
- Decision notice served – upheld
- Decision notice served – Partially Upheld

COM outcomes

- DC outside UK
- Not DPA
- No action for DC
- DC action required
- Improvement action plan agreed
- Undertaking served
- Advisory visit recommended
- Compliance audit recommended
- Enforcement notice pursued
- Civil monetary penalty pursued
- Criminal investigation pursued

ENF outcomes

- General advice given to org
- Compliance advice given org
- Monitored: sufficient improvement
- DC action required
- Improvement action plan agreed
- Undertaking served
- Advisory visit recommended
- Compliance audit recommended
- Preliminary enforcement notice served
- Criminal investigation pursued
- Enforcement notice served
- CMP notice of intent served
- CMP final notice served

Additional outcomes

All case types also have four 'marked for deletion' outcomes.

- Duplicate
- Documents pasted into existing case
- Non-CMEH
- Scanned in error

Descriptions of outcomes

- **DC outside UK** – Used when the data controller is outside the UK so the matter falls outside our jurisdiction. Concerns closed with this

outcome will be considered for possible referral to other DP authorities overseas using our international case-handling procedure.

- **Not DPA** – Used when it is clear from the information provided that the concern does not fall within the scope of the DPA, or it is not sufficiently clear whether the concern falls within the scope of the DPA. For example, where we cannot identify what, if any, personal information has been processed.

- **Concern to be raised with DC** – Used when a customer has raised a concern with us and we believe they should first have raised it with the DC. Should also be used in cases where the customer says they have raised the matter with the organisation responsible, but we need them to provide evidence (or more evidence) that they have done so, before we will deal with the matter.

- **Response needed from DC** – Used when a customer has raised their concern with a DC but a response has not been provided AND we believe the customer should either wait to receive it or do more to follow up their earlier contact with the DC. If a DC has not responded but we don't believe it is reasonable for the customer to have to follow it up (because their concern seems to be being ignored), we would deal with the case under a different outcome. We are likely to offer advice to the DC or expect them to take steps to improve their practices.

- **No action for DC** – Used when concerns raised by the customer do fall under the DPA because they are about the processing of personal information, but they are not valid because the data controller does not appear to have breached the legislation based on the information provided. We would not need to contact the DC but would provide advice to the DS. When applied to COM cases, we would use this outcome when the incident reported is not a breach of DPA or when a breach has happened but the organisation took all necessary steps and no practice improvements are needed.

- **General advice given to DC/org** – Used when the ICO wishes to contact a DC to offer advice about general information rights practice if their actions do not appear to have breached the legislation but a service improvement may have avoided the concern being raised with the ICO. ENF cases could involve providing advice under either DPA or PECR. The outcome reflects this by referring to the organisation rather than the data controller.

- **Compliance advice given to DC/org** – Used when no action is required of the DC but we do want to make them aware we have received a concern about them and are keeping it on file. This could be used where a DC put things right after a DS raised a concern with

them and the issue was minor, like correcting a single inaccuracy when prompted. ENF cases could be providing advice under DPA or PECR, so the outcome reflects this by referring to the organisation rather than the data controller.

- **DC action required** – Used when we identify an opportunity for the DC to take a one-off action to tackle a shortfall in their information rights practice where the action doesn't come within any other outcome category – such action may be, for example, providing a response to a customer's subject access request or engaging with a customer to address their information rights concern. When applied to COM cases, this outcome would be used if there is no opportunity to improve future practices but we do think a DC should take further action to deal with the reported incident. For example, the DC may need to contact those affected by the incident.

- **Improvement action plan agreed** –Used when we identify an opportunity to improve future practices and we either ask a DC to produce a plan to do this or we recommend that it should take particular steps to make improvements. Rather than one-off actions in individual cases, this outcome is used wherever we recommend ways to improve future practices on a broader level, such as reviewing processes or procedures to prevent concerns arising in future.

- **Monitored: sufficient improvement** – Used when we are satisfied that, after a period of monitoring, an organisation's practices have improved enough not to need further action.

- **Undertaking served** – Used when the ICO identifies specific actions for a DC to agree to improve future information rights practice.

- **Advisory visit recommended** – Used when we believe an organisation needs to improve practices, the most appropriate way to do this is to have an advisory visit, and Good Practice has agreed to approach them.

- **Compliance audit recommended** – Used when we believe an organisation needs to improve practices, the most appropriate way of doing this is to have a compliance audit, and Good Practice has agreed to approach them.

- **Enforcement notice pursued** – Used when it has been agreed to consider pursuing an enforcement notice and an ENF case has been created for this work to be progressed.

- **Preliminary enforcement notice served** – Used when a preliminary enforcement notice has been served.

- **Enforcement notice served** – Used when an enforcement notice has been served.

- **Civil monetary penalty pursued** – Used when we have agreed to consider pursuing a CMP and an ENF case has been created for this work to be progressed.

- **CMP notice of intent served** – Used when the ICO has issued a formal notice of intent to pursue a civil monetary penalty.

- **CMP final notice served** – Used when the ICO has issued a civil monetary penalty.

- **Criminal investigation pursued** – Used when we have agreed to investigate a criminal allegation and a PCB case has been created for this work to be progressed.

- **Insufficient information provided** – Used when the customer has not given us sufficient (or sufficiently clear) information to enable us to progress their case. This includes cases where the customer has not yet raised the matter with an organisation.

- **PECR does not apply** – Used when the matters raised do not fall under the PEC regulations.

- **Insufficient evidence of breach** – Although sufficient information has been provided, it remains unclear what information was processed/whether marketing material was sent by a particular organisation.

- **Enforcement not recommended** – Used when a PECR breach is confirmed but we will not take formal action.

- **Enforcement pursued** – Used when a PECR breach is confirmed and we will consider enforcement action.

- **Not PA** – Used when the organisation being complained about is not a public authority

- **Not s50** – Used when the matters raised are not eligible for consideration under s50 of the FOIA.

- **Not EIR** – Used when the matters raised are not eligible for consideration under the Environmental Information Regulations.

- **Vexatious** – Used when we deem the complaint vexatious.

- **Frivolous** – Used when we deem the complaint frivolous.

- **No internal review** – Used when no internal review has been engaged with/by the authority.

- **Undue delay** – Used when the complaint was raised with the ICO after an undue length of time.

- **Abandoned** – Used when, without prompting or negotiation, the customer informs us they no longer wish us to pursue their complaint.

- **Withdrawn informally resolved** – Used when, after negotiation with one or both parties, the customer agrees to withdraw their complaint.

- **Decision notice served – not upheld** – Used when ICO makes a decision that agrees with a public authority's handling of a request. The complaint is not upheld.

- **Decision notice served – upheld** – Used when ICO makes a decision that disagrees with a public authority's handling of a request. The complaint is upheld.

- **Decision notice served – partially upheld** – Used when ICO makes a decision that only partially agrees with a public authority's handling of a request. This should focus on the substantive issues rather than any procedural breaches.

- **Marked for deletion outcomes** – All cases with a 'marked for deletion' outcome will automatically be deleted from the system at set periods.

Actions providing closure states for multiple cases

There are some actions, such as undertakings and action plans, that can provide closures for more than one case. For example, if we send an undertaking to an organisation, and that undertaking relates to four cases, then the officer should make sure they close all four cases as 'undertaking served'.

Retention periods and rules for marking for preservation

CMEH automatically deletes closed cases two years after the last document was added to the case. However, we would like to retain certain types of case for longer.

Since November 2014, the Information Governance team has been responsible for all aspects of the process for identifying and marking cases on CMEH for permanent preservation and transfer to the National

Archives (TNA). Case Officers should not mark cases for permanent preservation for TNA purposes.

If case officers think a case should be retained for any reason other than permanent preservation at the National Archives, they should speak to their team/ group manager.

Re-opening cases

Some cases may come to us in two parts. For example, an individual may first tell us they have not received a response to a subject access request. If so, assuming there are no complicating factors, we will advise them to raise their concern with the organisation and close their case with the appropriate outcome recorded (that is, 'Closed – to be raised with DC').

If the individual returns to us with a further concern that is clearly related to the original one – for example, having now seen the information they requested, they are concerned it is inaccurate – we will re-open the original case, consider the second concern and then close the case recording the second case's outcome.

In terms of recording our work, we are viewing these two interactions with our customer as two separate but related concerns for them and against the organisation. Our re-opening of the case effectively creates a second case instance in CMEH under the same case reference number. The start date for that second case instance is the date we re-opened the case.

However, to make this approach work, we need to apply some important rules.

We must accept that the re-opened case state can only be used when we are creating a new transaction for a second, but related, concern. If, for example, we close a case and then need to change the original outcome, for example because we feel we may have initially selected the wrong one, we cannot simply re-open the case to do this. This is because it will be registered as a new piece of casework received by the ICO. Instead, the officer should report this to Operations Service Delivery who will amend the information in CMEH 'behind the scenes'.

We must also avoid closing and then re-opening a case within the same day. This can happen if we close a case because a customer has failed to give us enough information and the customer then provides it on the same day. If this happens, the officer should wait until the following day to reopen the case.

We will produce exception reports to indicate when a case has been closed and re-opened on the same day. Managers will be responsible for making sure these errors are kept to a minimum.
If we close a case with a given outcome but later receive more information from either party that causes us to reconsider but not change the outcome, there should be no change to the case state at any point. We should simply consider the new information without altering CMEH. This means this activity will not be measured. If, having considered the new information, we think it represents a further concern rather than a reconsideration of an earlier one, then we should re-open the case and treat the new information as a second but related concern as described above.

Creating new cases

A case officer may need to create a brand new case, for example where an individual's original concern turns out to be about two different organisations rather than just the one they originally mentioned.

When a case officer decides to create a new case, they should do so by following the procedures in the case manual section of the CMEH user guide.

12. Managing communications

Service adjustments

Case officers will use various methods to communicate with the parties to a case. However, they must take into account any 'reasonable adjustments' we have agreed to make or 'restricted contact' or 'single point of contact' arrangements we have made under our operating procedure ICO service adjustments: customers and our operating procedure on managing customer contacts.

Avoiding and managing inappropriate disclosures

Staff should also guard against the accidental or inappropriate disclosure of the personal information we hold and manage all external communications in line with the ICO operating procedure on Avoiding and managing inappropriate disclosures. Staff should also follow this operating procedure if an inappropriate disclosure of personal data occurs.

Welsh language scheme

When someone writes to us in Welsh we will reply in Welsh (if a reply is needed). Our target time for replying will be the same as for letters written in English.

Enclosures sent with Welsh letters should be Welsh or bilingual, when available.

Enclosures or attachments sent with bilingual letters should be bilingual, when available.

If a case officer receives a letter in Welsh, they should contact our Wales office for help. For more information, see our Welsh language scheme.

Outgoing communications

- **Telephone**

In most cases, we don't say how case officers should contact parties but we expect them to use the phone as much as possible.

A phone call can influence customers or stakeholders to respond positively. It can also be a much quicker way of conducting our business than letter or email and is often welcomed by our customers.

Even if a customer or stakeholder asks us to confirm our conversation in writing, our letter or email can be much more focused if we have phoned first. The call establishes a rapport and the following letter or email confirms the matters discussed or agreed. This tends to reduce the need for extensive secondary correspondence.

Sometimes we have to communicate in writing and a phone call may not always be practical, but case officers may close cases by phone, recording the outcome clearly in the 'contact history' section of CMEH (which allows for longer entries than the 'notes' page).

- **Email**

We are also keen to use email, as the fastest written communication channel, wherever possible. Sending regular casework material by email does not breach ICO security policy (see the Security manual - use of email for further information).

All emails to a party on a CMEH case on CMEH should be sent through CMEH. Case officers should not send case-related emails to customers or stakeholders from their 'personal' ICO email address (name@ico...). This helps ensure that a comprehensive set of case correspondence is available to view at all times. If case officers have to contact a customer or stakeholder privately, they should restrict access to the CMEH case. We do not expect case officers to need to do this often.

Sending all emails through CMEH also helps us maintain them in line with our retention schedule.

- **Fax**

There are some restrictions on sending email by fax. Please see our Security manual - use of fax for more information.

Incoming communications

- **Voicemail**

Customers are free to call case officers to discuss aspects of their case. Our phones have voicemail to take messages when staff members are unavailable because they are already on a call, are out of the office or are completing another task. Staff should only switch on their voicemail for one of those reasons.

Staff should also be active in managing their voicemail. If a customer calls and connects to an officer's voicemail, it is vital the outgoing message:

- is up to date,
- gives the staff member's name,
- says whether the staff member is in or out of the office, and
- says when they are likely to return the customer's call if a callback is needed.

If a member of staff is in the office on the day of the call, it is important the customer knows this from the outgoing message. If their call is urgent, this may discourage them from trying to contact other members of staff who are unaware of the details of their case.

Staff who are regularly out of the office will need to make a particular effort to ensure their voicemail messages are up to date. However, this doesn't mean they will have to re-record their messages every time they come back into the office.

Our system allows us to record two messages. It also allows us to set the date and time for one of these to automatically switch off. Used properly, and in line with the relevant instructions, it means that we never need to re-record our 'I'm in the office but away from my desk' message, and we never need to have to remember to switch off our 'I'm out of the office until x' message because the system does it for us.

Staff should also retrieve messages regularly and respond to them as promptly as they can. If homeworking and using ICO phone kit, they should not put off returning the call until they are back in the office.

- **Homeworking**

Staff working at home must comply with the ICO's homeworking policy, procedure and guidance. They must ensure they are as contactable by phone by colleagues and customers as they would be in the office. When working from home, officers should either:

- use the Softphone facility to connect to their office telephone via their homeworking kit and make and receive calls through their work telephone number, or
- use 'call forward' facility on their phone to forward calls to their home or mobile phone as appropriate, using the relevant instructions.

Staff should not set an 'out of office' email message and should ensure their calendars show they are working from home.

Staff should also include their direct-dial telephone number in all written correspondence they send to customers and stakeholders.

For more technical information about our phone system, please see the phone guide on ICON.

- **Calls to the helpline**

Although customers will usually have the case officer's direct-dial number, they may try to reach them through the helpline.

To help the helpline deal with such calls efficiently, case officers are responsible for the following:

- Taking calls when they are available – if a case officer can take a call they should do so, rather than asking the helpline to take or pass a message on.

- Keeping calendars up to date – if the case officer is not available, the helpline may need to arrange a callback, in line with the 'callbacks' section below. They will, however, always check the case officer's calendar first.

- Keeping voicemail messages up to date – as above.

- **No further contact (NFC) on cases**

There may be instances where a manager decides that we have given a customer all the information we reasonably can about a closed case and they therefore decide to restrict the customer's contact (in accordance with our 'Managing customer contact operating procedure').
Once the manager has explained to the customer that we will no longer speak to them about that particular case, the Case Officer should put 'NFC' into the CMEH case title. This will let any Helpline officer who may be speaking to that individual know that they shouldn't promise that anyone will call them back, although they can still say that they will let the relevant officer and/or manager know that they have called.

Requests for prioritisation

Where a customer rings the helpline to ask for a case to be prioritised, the adviser will simply tell them that they will pass on their request to the relevant manager, who will decide whether to prioritise the case at their

discretion. The adviser will also send a related email to the case, copying it in to the relevant manager, in case the case has not yet been allocated.

Callbacks on cases

If a party to a case tries to reach the case officer through the helpline and the person they need to speak to is unavailable, the helpline may need to arrange a callback. Case callbacks should take place within two working days, unless the customer agrees otherwise.

Callbacks on assigned cases

If a customer calls in relation to a case that we have assigned to a case officer and that officer is away from the office, the helpline will let the caller know, tell them when they will back and offer a callback within two working days of the officer's return.

If the caller will not wait that long, the helpline will attempt to contact the officer's manager and, if they are unavailable, arrange a callback from them within two working days. If the manager is also away, then the helpline will attempt to contact their manager, and so on, until they find someone who can return the call within two working days.

Callbacks on unassigned cases

If a customer calls in relation to a case that we have not yet assigned to a case officer, the helpline will try to put the call through to the relevant person (an LCO, Team Manager or Group Manager, as agreed locally with each sector team). If that person is away from the office, the helpline will try to contact their manager and so on. Again, the aim is to arrange a callback with someone who can return the call within two working days.

Signing off written communications

Information request paragraphs

Under the DPA and the FOIA, we are often asked for copies of the correspondence we send to and receive from third parties when doing to casework.

To help us deal with such requests, case officers should ask data controllers and public authorities whether there is anything in the information they send us, that they would not want us to send out if we were asked for it.

You should therefore include the paragraph below in any letter you send to a data controller or public authority, where you are asking them to provide information to help you deal with a case.

'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.'

Sign-offs

Case officers should sign off letters and emails as follows.

Name
Job title
The Information Commissioner's Office
01625 direct dial number

They shouldn't include department names as these are irrelevant to the customer.

Prisoner communications

The Information Commissioner's Office is included in the list of organisations which have "Confidential Access" when corresponding with prisoners. There is an associated procedure for confidential telephone conversations.

This policy applies to all prisoners throughout the UK, including Category A, young offenders and remand prisoners.

Accordingly, the procedure in Appendix 2 to this guide should be followed when sending correspondence to prisoners.

In addition, prisoners may make confidential telephone calls to the office. (Note: there is no provision for prisoners to receive confidential calls from the ICO.)

Documenting communications

Whenever contact is made by phone, case officers should consider whether they need to document any or all of what was said. Officers don't

need to log every call but they should record the details of calls in the following circumstances.

- Where the conversation is significant.
- Where the conversation relates to an ENF case.
- When closing a case by phone.
- When returning a call, or trying to return a call, arranged by the helpline.
- When a member of the helpline arranges a callback on a case, they will also email the officer concerned about the callback, sending a copy of that email to the case.

When making such notes, the officer should use the 'notes' section of CMEH or a 'Word' document if the note is particularly long.

If officers make hand written notes while on the phone (for example on a sticky note or a pad of paper) they must decide whether they should keep any of this information. If so, they should transpose it into the 'notes' section of CMEH before destroying the paper record.

When documenting communications, case officers should be careful to keep them factual and write in neutral, non-inflammatory language. If they use quotes, they should make sure they are accurate and clearly attributed.

Noting changes to contact details

- **Individuals**

If a customer notifies us of a change of contact details, the case officer is responsible for amending the details on CMEH in line with the relevant section of the 'party manual' section of the CMEH user guide.

- **Organisations**

The same applies to organisations, although Group Managers should also make arrangements for keeping accurate and up-to-date records of organisations most often contacted by their team, using spreadsheets in the 'party contacts' table on the 'organisations of interest' ICON page.

Dealing with follow up correspondence

There can be occasions when after a case officer has closed a case, one (or more) of the related parties contact them again, perhaps because they do not understand or agree with the decision they made.

In these circumstances, the officer should check to see if they can give any more information or clarification about their decision, and contact the person concerned one final time (in writing or over the 'phone), to see if they can help them better understand their reasons for making it.

We do not, however, expect case officers to get involved in protracted correspondence about closed cases. If the individual continues to write about the matter, the officer should let their manager know. The manager should then consider whether they can best deal with the matter as a complaint about our service [link to section 14 of manual]

Staff welfare

Occasionally, when our customers are unhappy with the service we have provided or are frustrated with their circumstances, they may behave in a way we find unacceptable or difficult to deal with. We have a legal obligation to protect the health and welfare of our staff and are committed to protecting and supporting any member of ICO staff who may encounter such behaviour.

Our Staff code of conduct requires that contact with our customers is always conducted to high standards. However, if any member of staff, when dealing with any ICO customer, feels threatened or distressed or has had any kind of difficulty when providing our service to customers, they should immediately bring this to the attention of their line manager or a more senior manager and consult our Managing customer contact operating procedure.

13. Support for progressing cases

Case officers can use a number of tools to help progress their cases.

Explanatory paragraphs

We have drafted some paragraphs explaining parts of our data protection casework service, which may be helpful when dealing with data protection concerns.

Because responses must fit the circumstances of the case, it won't necessarily be appropriate to repeat these explanations in full. Officers should use any paragraphs, sentences or phrases they think are useful and appropriate in the circumstances.

We sometimes receive requests for information we hold about cases and we usually have a duty under the FOIA to respond. Whilst it is in the public interest that we are open, transparent and accountable for the work that we do, it is important that we do not undermine the trust and confidence of those who raise concerns with us or of the organisations we regulate. We have therefore drafted a paragraph for case officers to include in their initial letters to data controllers, asking whether they have any reason why we should not share the information they send us in connection with the concern if we are asked for it.

Keeping it clear guide

The ICO has a number of clear communications principles. These are that our documents should:

- be accessible to the audience,
- be understood by the audience,
- influence the audience,
- inspire confidence in the audience, and
- be recognisable as ICO communications by the audience.

The keeping it clear guide gives tried-and-tested advice for writing effectively, style choices staff should make and common mistakes and tips on how to avoid them, which will help us fulfil those principles.

Policy advice and legal advice

Some cases may appear to raise novel or complex issues, where existing lines to take need clarifying or amending or new lines to take need to be produced. Other cases may require technical advice on legal issues about information rights law and other legislation.

In these circumstances, the case officer may need to seek spoken or written advice from Policy Delivery.

To request policy advice, please see the need some policy advice? pages on ICON.

To request legal advice, please see the policy delivery legal group pages on ICON.

However, before requesting advice from Policy Delivery, the case officer should check with their manager that the matter cannot first be resolved in the sector teams.

Information notices

Under the DPA, FOIA and PECR, if the Information Commissioner needs information to decide whether an organisation is complying with their obligations, he can serve an information notice (IN) requiring the organisation to give him the information. Failure to comply with an IN may be an offence.

If you feel that an IN may be required on a DPA case you are working, please see the factors to consider and factors to consider and procedure to follow in the Information Notice Procedure - DPA. If you decide to proceed with an IN, please use the Information Notice Request Form and Information notice covering letter.

If you think an IN may be necessary on a non-DPA case, please discuss this with your manager.

Process

- TBC

Special information notices

A form of information notice requiring an organisation or person to supply the ICO with information needed to ascertain whether personal data are being processed for the special purposes, namely journalism, artistic purposes or literary purposes (s44 of the Act).

Process TBC

Third party information notices

This is a form of IN requiring a communications provider to supply the ICO with information specified in the notice about another person's use of electronic communications when we need this to investigate a person's compliance with the PECR.

Information with protective markings

We sometimes need to see information an organisation has withheld from an individual. If case officers ask for this, the organisation will usually send it to them directly.

Case officers can ask the Scanning Team to scan it to the case if the information:

- does not conform to the description of 'physical evidence', and
- has a security classification of 'Official' or 'Official Sensitive'.

The ICO's core IT network can only process information or images of documents in the 'official' tier. If you have received or asked for information marked 'secret', you should contact the Information Security team for further advice. The ICO's physical security is not accredited to hold information marked as 'top secret'. The Scanning Team will not scan documents marked as 'secret' or 'top secret'.

In the unlikely event that withheld information reaches the Scanning Team without having been seen by the case officer, and the Scanning Team think it could be withheld information, the Scanning Team will contact the case officer to ask them to collect it.

If the case officer wants to return any 'withheld' information to the organisation, they should follow the process for returning documents to the individual [add link when we have final electronic version of guide]

Cases with media interest (non-DN cases)

Media-interest cases can be:

- cases that may generate media interest and therefore lead to an increased number of enquiries and concerns,
- cases we feel may be of media interest, e.g. where we'd like to issue a press release, or

- complaints submitted by a journalist where the outcome may be high profile.

Cases where the ICO has issued a decision notice will be identified as media-interest cases on the DN sign-off form.

If a case may be of media interest or be suitable for publication in our annual report, this is what to do.

- The case officer should ask their line manager whether the case they are closing may be of media interest.

- If it is, the case officer should tick the 'media interest' attribute when closing the case.

- The case officer should then complete the 'media interest' form:

    - saving it to CMEH case by emailing it to new.casework@ico.gsi.gov.uk including the wording 'MEDIA INTEREST FORM' and the case reference number in the subject field as follows [Ref. RFAXXXXXXX] or [Ref. FS50XXXXXXX]; and

    - copying the email to the OperationsServiceDelivery email address.

- A central record of these cases will be held by Operations Service Delivery. Details will go to our Communications Team, who will inform the ICO press office if necessary.

14. Feedback about our service

We make clear through the 'service standards and what to expect' section of our website that we value feedback about our service because it helps us improve. Customers and those we regulate can share their feedback with us by discussing matters with a case officer or sending them to us in writing.

Complaints directly from a party to a case

Such feedback can include complaints about how we have handled concerns or how we have treated parties to a case. Although we will try to deal with complaints made by phone, we may sometimes have to ask people to put them in writing, for example when we want to make sure we have a full record of the complaint in the complainant's own words.

In most cases, the case officer who dealt with the case will first check to see if they can resolve the complaint by giving more information or clarification about the decisions they reached.

If they can't do that, they will share the complaint with an appropriate manager, who will look at what we have done and why. The case officer should:

- set up a new RCC case, adding all relevant parties, documents and work items, in line with the CMEH user guide,
- on CMEH, link the RCC case with the case (or cases) the feedback relates to,
- acknowledge the complaint within five working days, and
- send it to the manager's queue.

When responding to a complaint, the manager should let the customer know that if they remain dissatisfied about our service, or they think we have not treated them properly or fairly, they can refer the matter to the PHSO, through an MP.

Timescales

Complaints must be made within three months of the incident the person wants to complain about. We will not usually consider late complaints. However, this is at the manager's discretion so the case officer should always inform them of a late complaint.

- We will acknowledge receipt of complaints within five working days.

- After considering the complaint, the manager will tell the complainant their decision within 30 calendar days of the complaint being raised with them.

Note – The threshold was reduced from six to three months on 1 April 2014. We will therefore take a flexible approach to applying the new threshold until October 2014. That is not to say we must work with the six-month threshold until then. If we have told a customer – in good time – that the threshold is three months, then that is the standard we should work to.

- **Disagreeing with FOIA decisions**

If someone disagrees with a decision notice we have issued about their FOIA complaint, they cannot complain under this process but must appeal to the First–tier Tribunal (Information Rights).

Complaints made through the PHSO

If, after we have considered their complaint, the complainant remains dissatisfied with our service, or thinks we have not acted properly or fairly, they can complain to the Parliamentary and Health Service Ombudsman (PHSO) through an MP.

Operations Service delivery (OSD) is the ICO's point of contact for the PHSO. The PHSO emails enquiries to the OSD inbox and the matter is processed as follows.

- An OSD officer creates an ENQ case, called 'PHSO enquiry'. The case will stay assigned to that officer.

- As the PHSO does not usually accept complaints until the individual has exhausted the relevant organisation's complaints process, we will usually have an RCC case relating to the matter. The OSD officer will link the ENQ case to the RCC case.

- The OSD officer will also add details to the OSD spreadsheet in Meridio.

- The OSD officer will contact the manager who conducted the RCC case, and put together any required responses. The OSD officer will also copy in the relevant Group Manager, if this is a different person.

- All internal e-mails regarding the PHSO enquiry and all correspondence to and from the PHSO should be added to the CMEH case.

Monthly figures will be collated for quarterly reporting to management board.

15. Other casework-related matters

Cases about the ICO

As a data controller and public authority, the ICO is subject to the DPA and the FOIA. If someone raises a related concern about us, we are still the statutory regulator and must deal with it as such.

These complaints will most likely arise as a result of the way we have dealt with:

- a DPA subject access request for information we hold,
- an FOIA request, and internal review, for information we hold, or
- the individual's personal data when providing them with one of our services (such as casework).

We will deal with such concerns in line with our usual procedures.

However, as our Information Access (IA) team handle most of our information requests, they are likely to receive any related concerns. In these cases, the IA team will be responsible for setting up the related cases on CMEH, to avoid any unnecessary delays on them reaching our systems. In all other instances, the case will be set up by the Advice Service.

Concerns about information requests – setting up the case

The officer will set up the DPA RFA or FOIA FS50 concern, adding the relevant parties and copying across relevant documents, as follows.

- **RFA**

- The original request.
- Their initial response or refusal.
- The concern or initial raising of concerns about the response or refusal.
- Their further response explaining the ICO position.

- **FS50**

- The original request.
- Their initial response or refusal.
- The request for internal review.
- The outcome of the internal review.

The officer will then:

- acknowledge receipt of the concern,
- refer the case to the correct CMEH team queue, and
- send an email to the relevant sector team, notifying them that the case has been added to their queue.

Concerns about information requests – progressing the case

After the concern has been allocated, the case officer should deal with it in line with our usual procedures. If they need more information from the ICO as the 'concerned about' party, they should not look at the related information request case and simply copy documents across, but should contact the relevant IA officer to discuss the matter.

Concerns about other(DPA matters

When the complaint relates to other matters, including casework, the case officer who dealt with that case will probably receive the complaint first through CMEH.

If so, the case officer should discuss the matter with their Group Manager, who will make sure we have provided the explanations we expect other data controllers to provide when an individual raises a DPA concern with them, and arrange to provide them if we have not.

If we have already provided such explanations and still receive a related concern, the case officer should:

- set up the RFA case on CMEH,
- add the relevant parties,
- add the relevant documents,
- send an acknowledgement, and
- let their Group Manager know we have received it.

The Group Manager will then make arrangements to deal with the matter, in line with our usual procedures.

ICO employee cases

ICO services are available to all members of the public. This means that ICO employees, as members of the public, may take advantage of these services personally or may know someone else who is.

Information about the progress and status of concerns and enquiries is available to a large number of authorised staff, particularly through CMEH. So we need to take extra steps to ensure that when casework is submitted by ICO employees, or by people known to them, we:

- protect their confidentiality, and

- ensure they do not access information about their case any sooner than if they were not an ICO employee or known to an ICO employee.

All ICO members of staff should follow this procedure when:

- submitting an enquiry or concern in their own name,

- they know of someone who has submitted casework to the ICO

- they are handling casework submitted to the ICO by a member of staff or someone who knows a member of staff,

- publishing performance information relating to our casework, or

- raising concerns about the handling of cases submitted under this procedure.

- **ICO staff submitting casework in their own name**

Where an ICO member of staff submits a concern or enquiry to the ICO, they should clearly mark their initial letter as an 'ICO staff case'.

If a matter is identified as an ICO staff case during the letter opening process, the correspondence should be passed straight to one of the Team Managers in the Advice Service (if possible, the Team Manager with responsibility for the sift). The Team Manager should then set up a CMEH shell case, with no reference to the content of the case, but with 'ECS' (for 'employee casework submission') in the title.

If a matter is identified as an ICO staff case during the inbox process, the material should not be placed on CMEH. Instead, the case officer should create a shell case with no reference to the content of the case, but with 'ECS' in the title, print the material from the inbox and then delete the electronic record. They should then refer the CMEH case to one of the Team Managers in the Advice Service (if possible, the Team Manager with responsibility for the sift) and pass over the hard copy material.

If a matter is identified as relating to an ICO staff case during the sift process, then the case officer should request the original hard copy of the information. Once they receive it, they should delete it from CMEH, making sure only a shell case remains, with no reference to the content of the case, but with 'ECS' in the title. They should then refer the CMEH case to one of the Team Managers in the Advice Service (if possible, the Team

Manager with responsibility for the sift) and pass over the hard copy material.

The Team Manager should then:

•identify the relevant Group Manager to deal with the matter,

•make sure that manager understands the procedure for handling such cases, and

•pass on the CMEH case and hard copy material to them.

The Group Manager of the relevant team should ask a Meridio administrator to set up a restricted access folder on Meridio to hold the case.

For cases to be dealt with in Improving Practice, the folder should be set up in the 'Improving Practice – Restricted cases' folder underneath 1.14.23. This is already restricted to the Performance Improvement 1-6 Group Managers Meridio group. By default, any folders added below this will inherit these permissions, so when requesting a new folder the Group Manager will need to confirm who also needs to access it (eg the case officer handling the case). The Meridio administrators will then send a link to each newly created folder to the case officer in question. They will have to access it through that link – as they will be unable to navigate to it in the fileplan as they won't have access to the 'Improving Practice – Restricted cases' folder.

The Group Manager responsible for progressing the case should ensure it is allocated to an appropriate officer or, if necessary, handle it themselves. If the manager considers a case to be particularly sensitive or has specific concerns about any conflict of interest, they should consult their head of department to decide whether to allocate the case to another team. The CMEH case should be updated with case state and nature/other attribute information, but all documents should be produced 'off CMEH' and held in the Meridio file.

If we need to write to another organisation to progress the case, we should give them the name of an individual to address their reply to and ask them to mark the envelope 'private and confidential'. If communication is to be by email, the manager should consider providing a personal email address. If they use 'Casework@' they should contact a Team Manager in the Advice Service to ask them to remove the electronic version from the outbox or inbox, as appropriate, providing the details they will need to find it.

Once the timeframe for related case reviews or service complaints has passed, the officer should delete the electronic records held on Meridio. Meridio will not destroy these records automatically and therefore the case officer is responsible for ensuring they have a process in place to ensure the deletion of these records takes place in accordance with the ICO records management policy.

If the subject matter was not identified as relating to an ICO staff case before the CMEH case was opened, the case owner must report this to their manager as soon as possible thereafter. Any case papers should be removed from CMEH and retained in a restricted access Meridio file, as described above. If the material was sent by post, the case owner should retrieve the originals from the scanning team. If it came by email, they should provide a Team Manager in the Advice Service (if possible, the Team Manager with responsibility for the sift) with the times, dates and addresses the emails were sent from, so they can delete them from our inbox. Prior to formally allocating the case to a case officer, the Group Manager must ensure that that member of staff understands this procedure.

- **If ICO employees are aware of someone they know submitting casework to the ICO**

If you know of a case being submitted to the ICO and feel that, given your area of work, you may be asked to handle it, you should alert your line manager to ensure any potential conflict of interest can be avoided.

However, if you are unlikely to be involved in handling any such casework but would have access to information about it through CMEH, then you must avoid accessing such information unnecessarily. Refer to the 'Staff confidentiality' section of this procedure.

Staff who access information without good cause or breach the confidentiality clause in their contract of employment may be subject to formal disciplinary action.

- **Staff who handle complaints submitted by ICO employees**

Any member of ICO staff who handles casework submitted by ICO staff will do so in strictest confidence. The case will not be discussed with any members of ICO staff who do not have a legitimate need to be involved. The employee/customer will not be given access to any information they would not be entitled to as a regular ICO customer.

- **Publishing our casework performance**

The ICO publishes some details internally about our casework performance, which can include the name of customers. When casework has been submitted by an ICO employee and we need to publish details of the case, they will be referred to by the ECS reference number.

- **Concerns about keeping to this procedure**

If any member of ICO staff has reason to believe that this procedure has not been followed, they should report it to the Operations Service Delivery Group Manager.

- **Duty of confidentiality**

When keeping to this procedure all ICO staff are reminded of the confidentiality clause that is fundamental to their contract of employment. This clause states:

"As an employee you will have access to both personal data and other information held by the Information Commissioner and will therefore be bound by a duty of confidentiality in respect of all such information which comes into your possession. Any disclosure may constitute a criminal offence contrary to s59(1) of the Data Protection Act 1998 for which you will be personally liable."

Whistle-blowers

If a customer is concerned that their employer may be contravening information rights legislation, they may contact the ICO.

If they are concerned that disclosing this information to the ICO may lead to them being penalised by their employer, they may be protected by whistle-blowing provisions of employment-rights legislation.

The ICO cannot advise whether a disclosure would be protected. The customer must satisfy themselves about this. However, we have produced our 'Protection for whistle-blowers disclosing information to the ICO', which potential whistle-blowers should be made aware of.

In most cases, our contact with whistle-blowers will be through the Advice Service. If casework staff become aware of a potential whistle-blowing case, they should contact a manager in the Advice Service.

Appendix 1 – Terminology

Advice Service – Part of our Customer Contact Department. Responsible for the initial receipt and sift of most incoming correspondence to the Operations directorate. It also responds to requests for written advice and provides the ICO's national Helpline service.

assessment – A decision made under s42 of the DPA as to whether it is 'likely' or 'unlikely' that the processing of personal data has been carried out in compliance with the DPA.

cases – All new requests made of the ICO Operations Directorate by a customer. All cases are held on CMEH.

case types – All cases have a 'type' based on how we want to describe and measure the work involved.

classifying work – Giving work a case type on CMEH.

case attributes – In each 'case type', there are 'attributes' describing the nature, sector and other relevant information about the case.

case officer/officer – The primary ICO staff member working on case, whatever their grade.

case outcomes – Every case has a specific 'outcome' recorded when it is closed.

CCA – The Consumer Credit Act 1974

civil monetary penalty – The ICO can issue fines of up to £500,000 for serious breaches of the DPA and PECR.

CMEH – The ICO's electronic casework management system.

customer – Anyone who contacts us to access our services.

data controller (DC) – Legal 'person' subject to the DPA.

data subject (DS) – Individual protected by the DPA.

DPA – The Data Protection Act 1998.

decision notice (DN) – A formal decision outlining the Commissioner's view as to whether or not a public authority has complied with the FOIA or the EIR with regard to a specific complaint.

EIR – The Environmental Information Regulations 2004.

FOIA – The Freedom of Information Act 2000.

ICO – The Information Commissioner's office. The UK's independent public authority set up to uphold information rights.

information asset register – List of information physically held in hard copy (in the case of paper documents) or some other form (e.g. memory sticks)..

information notice (IN) – A notice requiring an organisation or person to supply the ICO with the information specified in the notice for the purpose of assessing whether the Act or related laws have been complied with. Failure to comply with a notice is a criminal offence.

IRC – The ICO's Information Rights Committee. The part of the ICO's formal governance framework with responsibility for setting our regulatory and information rights priorities.

ODDH – The Operations Directorate Departmental Heads. The team of ICO senior managers with overall responsibility for the Operations Directorate.

Operations Service Delivery Group – Supports the activities of the Operations Directorate, providing management information and project management among other things.

organisation/stakeholder – Those the ICO regulates.

Parliamentary and Health Service Ombudsman (PHSO) - Investigates complaints from individuals that they have been treated unfairly, or have received poor service, from government departments, other public organisations and the NHS in England. This includes the ICO. Complaints must be made through an MP.

parties – Every case has 'parties' linked to it. These are the person or organisation making the contact with us and the organisation they are concerned about, where this is relevant.

PECR – The Privacy and Electronic Communications (EC Directive) Regulations 2003.

Performance Improvement Department (PID) - Part of our Operations directorate handling concerns raised under DPA, FOI, and EIR

PhonepayPlus – The regulator for premium-rate (or phone-paid) services in the UK.

physical evidence – Items sent in connection with an information rights concern which can't or won't be scanned to CMEH, such as discs, DVDs and large lever-arch files of cross-referenced documents.

protectively marked information – protective marking is a system used to protect information from intentional or inadvertent release to unauthorised readers. Sensitive information is classified into a number categories, which indicate the level of protection that is required.

public authority – Bodies subject to the FOIA.

sector groups/teams – The ICO has six sector-focused groups containing a number of teams. They report into the Performance Improvement Department and the Customer Contact Department. The sector teams are responsible for dealing with the information rights concerns the ICO receives.

self-service – The steps we usually expect individuals to take to resolve an information rights problem with the organisation that was responsible for it, before bringing the matter to us.

Scanning Team – Part of Operations Service Delivery. Responsible for scanning documents to CMEH, securely destroying documents in line with our retention policy and managing some paper records until collected by the relevant case officer.

self-reported incidents – Potential breaches of the DPA, reported by the organisation responsible for it.

TPS – Telephone Preference Service. A non-statutory telephone marketing 'opt-out' service.

TSP – Telecommunications service provider.

undertaking – A formal document that commits an organisation to a particular course of action in order to improve its information rights compliance.

whistle-blower – A person concerned that their employer may be contravening information rights legislation and brings it to our attention.

work items – 'Work items' are actions associated with a case. It is the 'work item' that sits in the work queues. One case may have more than one 'work item' underway at any one time, though this is uncommon. In

most cases one member of staff will do one item of work to progress or close each case at any given time.

work queues – For work to flow through the organization, we use 'work queues' in CMEH. These work queues belong to the groups and teams across the directorate. The work queues have assigned to them the work needed to progress and complete each case.

Appendix 2 – Related policies, procedures and resources

All staff should take time to familiarise themselves with these additional related policies, procedures and resources.

Avoiding and managing inappropriate disclosures

Cases of media interest (FOIA)

CMEH user guide

Data protection regulatory action policy

Document retrieval process

Freedom of information regulatory action policy

Helpline directory

High profile case procedure

Homeworking policy, procedure and guidance

ICO operating policy - employee casework submissions

ICO Reasonable Adjustment Policy

ICO service adjustments: customers

ICO translation policy

Inbox procedure (see sift manual, appendix 7)

Sectoral responsibilities spreadsheet

Information notice procedure - DPA

Information rights concerns - guidance for organisations

International enforcement co-operation - instructions for checklist

International enforcement co-operation - checklist

Keeping it clear guide

Managing customer contacts

Media interest form

Need some policy advice?

Notification of data security breaches to the ICO

Opportunity assessment framework

Organisations of interest

Phone guide

Physical evidence process

Policy delivery knowledge base

Policy delivery legal group

Prisoner communications policy

Protection for whistle-blowers disclosing information to the ICO

Raising information rights concerns – guidance for individuals

Raising information rights concerns – guidance for organisations

Raising information rights concerns effectively (webpage)

Reasonable adjustments database

Report your concerns tool

Restricted contact database

Retention and disposal - preservation criteria - casework

Return of original documents process

Scanning performance updates

Security manual

Security breach notification form

Service standards and what to expect

Signing off a case with a decision notice process

Notification of data security breaches to the ICO

Sift manual

Single point of contact database

Staff code of conduct

Standard (FOIA) casework guides, forms and letters

Undertakings guidance (currently being amended)

Welsh language scheme

Withheld, confidential, secret and top secret information processes

Working with other bodies

Appendix 3 – Service standards and relevant timescales

- We scan and acknowledge paper correspondence representing new cases within 24 hours of us receiving it. Emails are acknowledged automatically as soon as they arrive.

- All cases – except for self-reported incidents – should be assigned to the relevant sector team work queue no later than three working days after the case was created in CMEH.

- Self-reported incidents should be assigned no later than five working days after being created in CMEH, to allow for the Enforcement triage of this work.

- We aim to fulfil the requests of 90% of customers asking for written advice within 14 calendar days and the rest within 30 days. If customers give us a daytime telephone number, we will try to contact them sooner.

- When customers provide clear 'self service' replies, we will contact them within 30 calendar days, giving advice about how we think the law applies to their issue or concern, where appropriate.

- We aim to close 90% of cases about concerns within six months.

- We will return calls about cases (assigned or unassigned) within two working days, unless the customer agrees otherwise

- Complaints about our service must be made within three months of the incident the person wants to complain about. We will not usually consider complaints made later than this.

- We will acknowledge receipt of complaints about our casework service within five working days.

- If the person who dealt with the customer cannot resolve a complaint by providing further relevant information, they will share the complaint with a manager. The manager will consider the matter and reply within 30 calendar days of the complaint being raised with them.

- Responses to correspondence from elected representatives should be drafted within 10 working days of receipt into the office.