Information Access Manual

Document name	Information Access Manual
Version number	1.1
Status	Published
Department/Team	Information Access
Relevant policies	N/A
Distribution	Internal
Author/Owner	Information Access
Approved by	Louise Byers
Date of sign off	30 June 2023
Review by	30 June 2024
Security classification	Official

Contents

Foreword

The role of the ICO's Information Access Team is pivotal in ensuring that the ICO complies with the legislation it regulates. Amongst other duties, we are responsible for responding to requests for information that we hold. 2022 marked a turning point for our team. Following successful completion of our recovery plan the team has been able to turn its attention to important projects that support our compliance with information rights legislation. As information rights practitioners at the ICO we hold a unique position in the field, and we recognise that other organisations look to us to set an example in our management of information requests and the service we provide to our requesters.

This, coupled with the strategic objectives set out in the ICO25 plan, in particular to promote openness and transparency, and to continuously develop the ICO's culture, capability and capacity, has led the team to consider what we can do to embody these principles. As a newly expanded team, with varying levels of experience, the team has recognised that there was an opportunity to review, clarify and improve the way in which Information Access operates. This has been done through collating sources of existing guidance and producing new resources where previously, locally held knowledge had been relied upon. The result is this manual. It is intended to be used as a tool to support the team and promote best practice in our request handling procedures alongside our existing guidance. I am very grateful to those who contributed to its development and recognise the importance of this work to the future success of the team.

The manual you see here is not a complete and finished work. It is intended to be a living document, which will evolve over time as the Information Access Team identifies improvements and more efficient ways to operate. The manual will be updated to reflect these changes over time.

Information Access is an ambitious team – determined to respond to every request on time, in line with the public commitments made by the Information Commissioner. This manual is a tool to support the team in achieving that target and to support the induction of new team members, and I hope you will find it useful as you progress through your career within the Information Access Team.

Louise Byers
Director of Risk and Governance
ICO Data Protection Officer

Acronyms & Terminology

Acronyms and terminology you may encounter during your work in IA and throughout this document.

Acronym / Term	Stands for / Meaning	Notes
AI	Access to ICO Information	IA area of SharePoint
BAU	Business As Usual	
BCR	Binding Corporate Rules	
CMA	Competition and Markets Authority	Non-ministerial government department
CMEH	Old ICO casework system, no longer used	
COB	Close of Business	
CREAP	Communicating our Regulatory and Enforcement Activity Policy	ICO policy
CRIT	Criminal Investigations Team	ICO team
DC	Data Controller	
DCMS	Department for Culture, Media and Sport	Former sponsoring department of ICO
DL	Disclosure Log	
DP	Data Protection	

Acronym / Term	Stands for / Meaning	Notes
DPA	Data Protection Act	2018 legislation
DPIA	Data Protection Impact Assessment	
DPO	Data Protection Officer	
DN	Decision Notice	
DPDI	Data Protection and Digital Information Bill	Potential new DP legislation
DRCF	Digital Regulation Cooperation Forum	CMA, Ofcom, ICO, and FCA
DS	Data Subject	
DSIT	Department for Science, Innovation and Technology	Current sponsoring department of ICO
DSP	Digital Service Provider	
EDPB	European Data Protection Board	
EDRM	Electronic Document and Records Management	ICO uses SharePoint as its EDRM
EIR	Environmental Information Regulations	2004 legislation
EOD	End of Day	
ET	Executive Team	
FCA	Financial Conduct Authority	UK Regulator

Acronym / Term	Stands for / Meaning	Notes
FDA		One of the unions recognised by the ICO
FOI	Freedom of Information	
FOIA	Freedom of Information Act	2000 legislation
FOISA	Freedom of Information (Scotland) Act	2002 legislation
FRU	Financial recovery unit	ICO team
FS50	FOIA s50	How the IA Team refers to FOI complaints
FTT	First Tier Tribunal	
GAFAM	5 big tech companies (Google Apple Facebook Amazon Microsoft)	
GM	Group Manager	ICO job role
GPA	Global Privacy Assembly	International Forum
GRA	Gender Recognition Act	2004 legislation
GRC	Gender Recognition Certificate	
HP	High Profile	Qualifier used in IA case summaries
HPI	High Priority Investigation	
HPIPP	High Priority Investigation Policy & Projects Team	ICO team

Acronym / Term	Stands for / Meaning	Notes
HTC	How to Complain	DP complaint case summary shorthand
IA	Information Access	
IAM	Information Asset Manager	
IAO	Information Asset Owner	
IAR	Information Asset Register	
IASO	Information Access Support Officer	ICO job role
IR	Information Rights or Internal Review	
Iris	The ICO Intranet	
KP	Knowledge Pack	
LAA	Local Asset Administrator	
LBA	Letter Before Action	
LED	Law Enforcement Directive	
LIAO	Lead Information Access Officer	ICO job role
LIMO	Local Information Management Officer	
LTT	Lines To Take	
MM	Mail Management	Qualifier used in IA case summaries

Acronym / Term	Stands for / Meaning	Notes
MMD	Multimedia Device	Laptop
MPN	Monetary Penalty Notice	
NCND	Neither Confirm Nor Deny	
NCOB/NCB	Normal Course of Business	
NCSC	National Cyber Security Centre	UK Authority for Cyber Threats
NFA	Not For Action / No Further Action	
OBO	On Behalf Of	
Ofcom	Office of Communications	UK communications regulator
OSD	Operations Service Delivery	
OOO	Out of Office	
OSR	Open Source Research	eg Googling
PA	Public Authority	
PACE	Prioritise, Act, Collaborate, Engage	ICO project team type
PACE	Police and Criminal Evidence Act	1984 legislation
PADPCS	Public Advice & Data Protection Complaints Service	ICO department

Acronym / Term	Stands for / Meaning	Notes
PCS	Public and Commercial Services Union	One of the unions recognised by the ICO
PD	Personal Data	
PDB	Personal Data Breach	
PDMIT	Privacy and Digital Marketing Investigation Team	ICO team
PECR	Privacy and Electronic Communication Regulations	2003 legislation
PETs	Privacy Enabled Technology	
PGA	Parliamentary and Government Affairs	ICO department
PIT	Public Interest Test	
RA	Reasonable Adjustment	Qualifier used in IA case summaries
RAP	Regulatory Action Policy	ICO policy
RC	Restricted Contact	Qualifier used in IA case summaries
RDSP	Relevant Digital Service Providers	Register held by ICO
RoPA	Record of Processing Activities	
RPSI	Re-use of Public Sector Information Regulations	2015 legislation
SAR	Subject Access Request	

Acronym / Term	Stands for / Meaning	Notes
SCC	Standard Contractual Clauses	
SIAO	Senior Information Access Officer	ICO job role
SIRO	Senior Information Risk Owner	
SLT	Senior Leadership Team	
SPOC	Single Point of Contact	
TM	Team Manager	ICO job role
TNA	The National Archives	Non-ministerial government department
Touchpoint		ICO live chat and helpline system
TULRA	Trade Union and Labour Relations (Consolidation) Act	1992 legislation
UTT	Upper Tier Tribunal	
VM	Voice Mail	
WDTK	WhatDoTheyKnow.com	Website for making FOI requests

Section updated: 19 February 2024.

Request Handling

Introduction

Every information rights request that we handle is different. As such, this manual cannot, and should not, explain exactly how to approach every single information request. Each request case must be considered individually.

This chapter contains information on the key points in the life of the most typical information requests; subject access requests, and Freedom of Information requests. Not all pages in this section will be relevant to every request received by the Information Access Team – it may be that on a straightforward request, you need to refer to very little. When requests involve more detailed handling, such as finding information in ICE 360, or consultation, you will find the guidance here.

ICE 360 Overview

ICE 360 is the ICO casework management system for IA, PADPCS, FOI Complaints, and the PDB team. It replaced the previous system, CMEH. It is based on Microsoft Dynamics software, and it is integrated with SharePoint so documents you see in ICE 360 are actually held in SharePoint (but are not searchable there).

Functions

1. Emails can be sent directly into ICE 360 via icocasework@ico.org.uk (for complaints, advice or PDB reports) or icoaccessinformation@ico.org.uk (for information requests). Only IASOs should use the latter in order to create cases once they have been triaged.
2. If a complete case reference is included in the subject line the email will automatically attach to that case.
3. If more than one case reference is in the subject line, the email will only attach to the first case listed.
4. New emails and cases assigned to you will appear on your ICE 360 dashboard.
5. Unassigned cases and emails will appear in Queues. Emails sent to icoaccessinformation@ico.org.uk will go to the 'IR Queue'. IR stands for Information Rights, and is the queue for the IA Team in ICE 360.
6. All emails and documents associated with each case should be stored on the relevant case in ICE 360.
7. A case Snapshot can be created. This is a PDF file of all documents and emails attached to a case.
8. Documents and draft, unsent emails attached to a case can be deleted by any user. However, to have a sent or received email deleted from a case you need to contact IT Help.
9. Consult ICE 360 Manual and IA ICE 360 Case Handling Procedure for more on using ICE 360 for casework.

Other resources: ████████████████████████ ICE 360 support files.

████████████████ - Documents for ICE 360 guides.

Search Workday for more in-depth training on using ICE 360.

Section updated: 13 April 2023.

Managing Your Caseload and Request Tracking

Task

Managing ongoing cases, deadlines and consultations.

Steps

1. Your ICE 360 dashboard highlights your ongoing cases, received emails and unsent, draft emails.
2. You can also consider using your own case tracker in the form of a spreadsheet.
3. Your tracker could cover the following:
    a. The case due date.
    b. The status of scoping – whether it is ongoing or completed.
    c. Whether any internal or external consultations are required.
    d. The due dates of any ongoing consultations.
4. You may wish to keep notes about a case with this tracker. For example, questions you have for Request Queries sessions, or any exemptions used. However, ensure that any information on the tracker is also contained on the relevant ICE 360 case record. Relevant information regarding the handling of a case should be present on ICE 360.
5. As with all information created, consider that information on your tracker may be disclosable under information rights legislation.
6. As soon as your request case is completed it should be deleted from your tracker.

Other resources: ███████████████████████████████ Template Request Tracker.

Section updated: 17 May 2023.

Subject Access Requests Checklist

Task

Processing and responding to all subject access requests (SARs).

Checklist

1. Is the request clear? Ask for clarification if not. See ███████████████████████████████, for templates. Pause the clock on the timeframe for our response until clarification is received. Update ICE 360 due date accordingly, and advise the requester of the new deadline.

2. Are you confident of the requester's identity? If not, ask for ID. See ████████████████████ ████████, for templates. The timeframe for our response starts when ID is received. Update ICE 360 due date accordingly, and advise the requester of the new deadline.

3. Is the request particularly complex or voluminous? Ask for clarification if needed, and pause the clock on the timeframe for our response, or extend the deadline by two months. Update ICE 360 due date accordingly, and advise the requester of the new deadline.

4. Is the request on behalf of someone else? Do they have authorisation from the data subject. If not, ask for authorisation. The timeframe for our response starts when authorisation is received. Update ICE 360 due date accordingly, and advise the requester of the new deadline.

5. Does the requester have a reasonable adjustment, a single point of contact, or are they on restricted contact? Check the Service Adjustments list.

6. Is the request a repeat, or potentially manifestly unfounded? Check earlier cases for a previous warning or the same request.

7. Have they requested our response in a particular format? If so, send the response in that format if reasonable to do so.

8. Are you sending the response as a hard copy by post? If so, send Recorded Delivery.
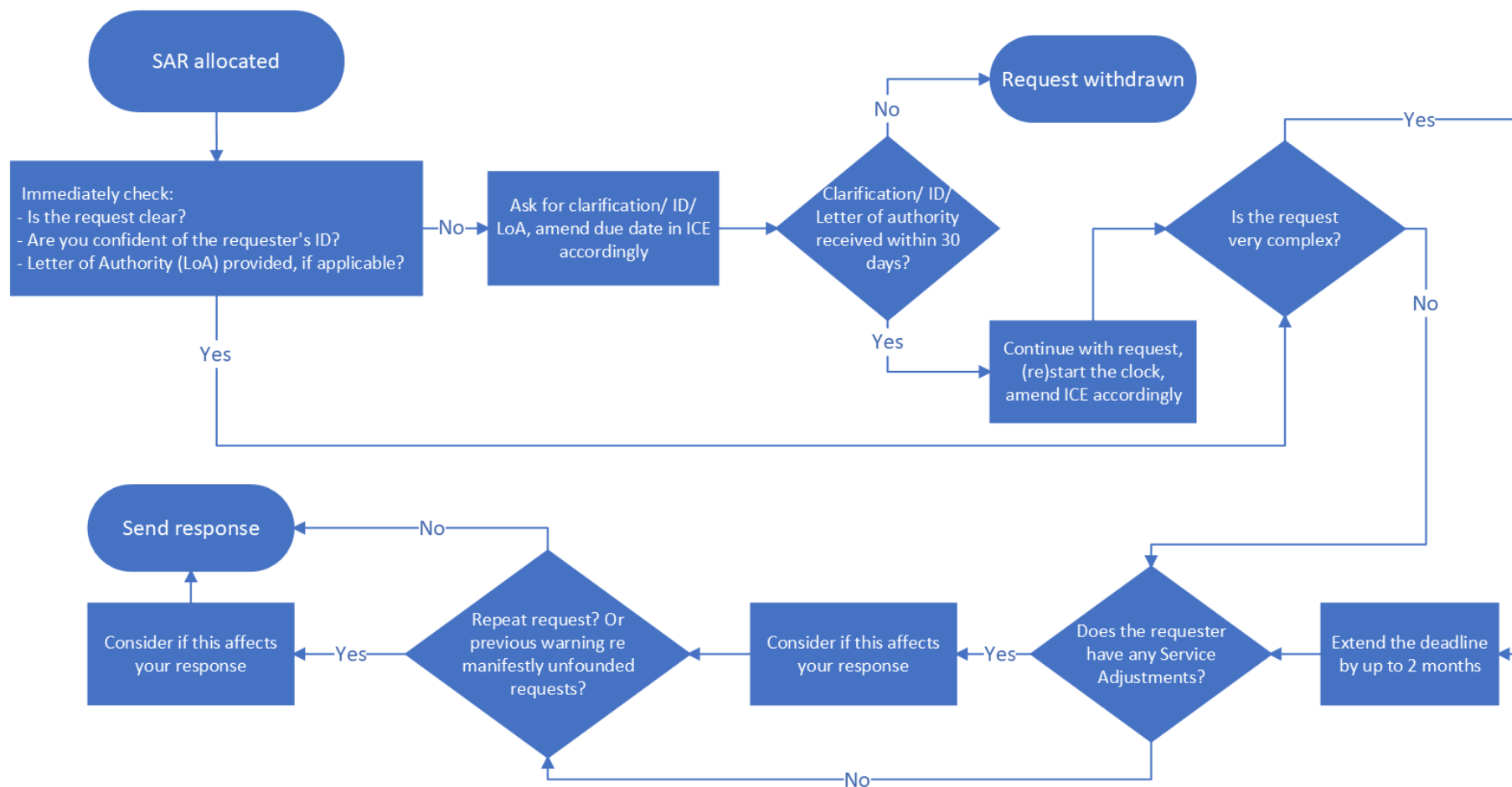
Other resources: ICO website - Right of access.

Section updated: 26 October 2022.

Scoping Subject Access Requests

Task

Finding all relevant information when responding to SARs. Not all of the following will be relevant to every SAR, and the list is not exhaustive.

Steps

1. Are you confident of the identity of the requester and how to identify their personal data? Ask for ID, a letter of authority and/or more information if not. See ███████████████████████████████, for templates.
2. Consider if the requester has multiple contact records in ICE 360. Have they used more than one email address during a complaint? Are you confident that different contact records are for the same person?
3. Check for previous SARs from the requester in ICE 360 and in CMEH Legacy. We do not need to provide information already given under a previous SAR.
4. Out scope information already exchanged with the requester, unless they have specifically asked for something they have sent to us or we have sent to them and it is reasonable to provide it.
5. Consider if you need to consult individual case officers to see if they hold any information in scope outside ICE 360 eg internal communications via Outlook, Teams, case reviews, service complaints etc.
6. Consider if you need to check our Live Chat service – live chat transcripts are retained for 100 days. A limited number of the IA Team can access Touchpoint Reports to check for transcripts.
7. Consider if the requester appears on the Service Adjustments list, Terminated Contact Logs, or other SharePoint documents, and if such information is in scope.

Section updated: 15 February 2023.

FOI Requests Checklist

Task

Processing and responding to all FOI requests.

Checklist

1. Is the request in writing? If not, send back to the referring colleague. The requester must make the request in writing unless they have a specific Reasonable Adjustment already in place.
2. Do we have a name and means of providing our written response? Ask for a name and email/postal address if not. A social media handle is sufficient. The statutory timeframe for our response starts when these are received. Update ICE 360 due date accordingly, and advise the requester of the new deadline.
3. Is the request clear? Ask for clarification if not. See ███████████████████████, for templates. The statutory timeframe for our response starts when clarification is received. Update ICE 360 due date accordingly, and advise the requester of the new deadline.
4. Have you searched completed cases in ICE 360 for similar requests that may inform your response?
5. Have you searched the [ICO Disclosure Log](#) for similar requests that may inform your response?
6. Consultation required? Do consultations as soon as possible to allow time for consultees to respond, and allow time for you to consider the information they provide, and their views on disclosure.
   a. Internal consultations? Check ██████████████████████████████████ Team contacts for requests to ICO, for who to consult.
   b. External consultation? Add the consultee to Contacts and/or Accounts in ICE 360.
7. Do you need more time to consider the Public Interest Test (PIT)? If so, extend the timeframe for our response accordingly, and notify the requester using the PIT Extension Generic template. Update ICE 360 due date accordingly.
8. Does the requester have a reasonable adjustment, a single point of contact, or are they on restricted contact? Check the Service Adjustments list.

9. Check if the requester has received warnings regarding repeated or vexatious requests. Consider if this impacts on your response.

10. Have they requested our response in a particular format? If so, send the response in that format if reasonable to do so.

Other resources: ICO website - Guide to freedom of information.

Section updated: 24 November 2022.

Scoping FOI Requests

Task

Finding all relevant information when responding to FOI requests. Not all of the following will be relevant to every FOI request, and the list is not exhaustive.

Steps

1. Check for previous similar requests using the ICE 360 filtering function (search keywords in the case summary) and using the keyword search in the ICO Disclosure Log.
2. Search relevant organisations using the Accounts search in ICE 360.
3. Use ███████████████████████████████████ Team contacts for requests to ICO to understand if there are other ICO departments you should consult.
4. Search keywords using the SharePoint search function.
5. Scoping *open* FOI complaint cases – consult the complaint Case Officer as they may hold information outside ICE 360, and may have views on disclosure.
6. Closed PDB cases, no investigation pursued – all relevant information will be in ICE 360.
7. Closed PDB cases, investigation pursued – a separate case reference will be held in the Crimson spreadsheet. Ask an SIAO to check CRIMSON re investigation case reference and investigating officer (ie who to consult).
8. Consider if we have or will soon proactively disclose the requested information by checking the Our information section of the ICO website, eg Datasets.
9. If the request involves corrective measures taken by the ICO (ie Penalty Notices, Enforcement Notices, Information Notices, Assessment Notices, Warnings, Reprimands, or Prosecutions), consider the Corrective Measures Spreadsheet that records these measures. A designated SIAO will have access to this.

Section updated: 13 December 2022.

EIR Checklist

Task

Processing and responding to all Environmental Information Regulations requests.

Checklist

1. Is the request for environmental information? Review ICO guidance on [Regulation 2(1) - What is environmental information?](#) if you are unsure. If the information requested is environmental information, process as an EIR request. If it is not environmental information, process as an FOI request.
2. Note that in contrast to the FOIA, an EIR request can be made verbally.
3. Do we have a name and a means of providing our written response? Ask for a name and email/postal address if not. In contrast to the FOIA, the requester does not need to use their real name.
4. Is the request clear? Ask for clarification if not. Under EIR, if a request is too ambiguous or general, you have 20 working days to ask for further information. The statutory timeframe for our response starts when clarification is received. Update ICE 360 due date accordingly, and advise the requester of the new deadline.
5. Have you searched completed cases in ICE 360 for similar requests that may inform your response?
6. Have you searched the [ICO Disclosure Log](#) for similar request that may inform your response?
7. Consultation required? Do consultations as soon as possible to allow time for consultees to respond, and allow time for you to consider the information they provide, and their views on disclosure.
    a. Does the request require internal consultations? Check ████████████████████████ ████████████████████████ Team Contacts document for who to consult.
    b. Is external consultation required? Add the consultee to Contacts and/or Accounts in ICE 360.
8. Do you need more time to respond to the request? Under EIR, you can extend the timeframe for a request by an additional 20 working days if the request is particularly voluminous or complex. If you are unclear as to whether a request meets these criteria, review ICO guidance on [Time limits for compliance](#)

under the Environmental Information Regulations 2004. If you extend the timeframe, you will need to notify the requester and update the ICE 360 due date accordingly.

9. Does the requester have a reasonable adjustment, a single point of contact, or are they on restricted contact? Check the Service Adjustments list.

10. Check if the requester has received warnings regarding repeated or manifestly unreasonable requests. Consider if this impacts on your response.

11. Have they requested our response in a particular format? If so, send the response in that format if reasonable to do so.

Other resources: ICO website - Guide to the Environmental Information Regulations.

Section updated: 16 May 2023.

Searching ICE 360

Task

Finding information in ICE 360 using the global search function, local search function, and keyword searching.

Global Search Function

1. The global search function in ICE 360 is in the blue ribbon at the top of the screen.

2. Click the white magnifying glass icon > enter a search term > press Enter.
3. This searches all areas of ICE 360 for the inputted search term. For example, if you search for a case reference using the global search function it will show the relevant case in the results but also all emails (activities) that quote that case reference.
4. You can filter the results by area (Contact, Activity etc) using the Filter drop down in the top right.
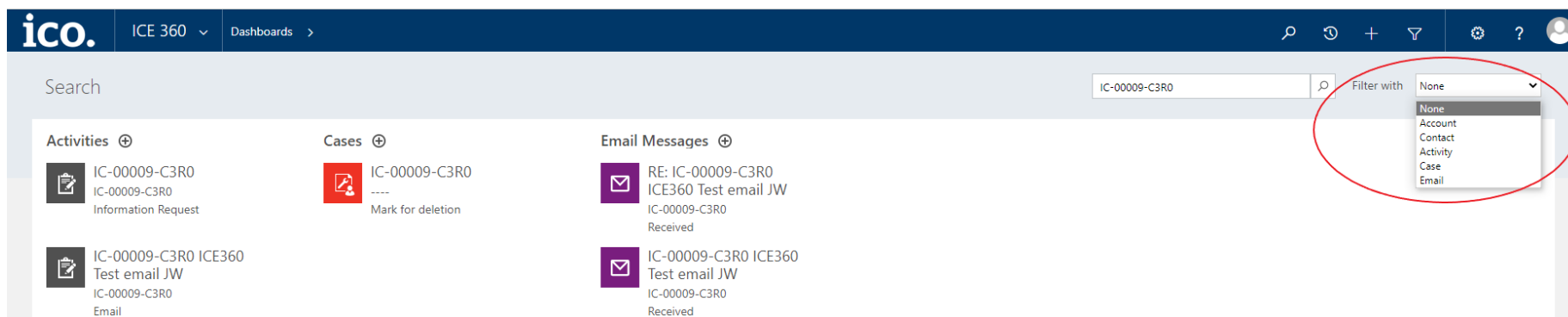
5. When searching for a specific case using the global search function, search only for the numbers in the centre of the case reference as this will produce much quicker results, eg if the full case reference is 'IC-123456-A1B2', just search for '123456'.

6. As this search function searches all of ICE 360 it can be very slow and produce irrelevant results. If you are searching for a specific type of information (a contact record, a specific case etc) use the local search function.

Local Search Function

1. The local search function in ICE 360 is in the grey ribbon towards the top of the screen. It does not appear when in your main dashboard, or a specific case, contact or account record.

2. Enter a search term in the white box > press Enter.

3. This searches for the inputted search term in that specific area of ICE 360. For example, if you use the local search function when in the 'Cases' area, it will only look for your search term within case references, sector and case outcome.
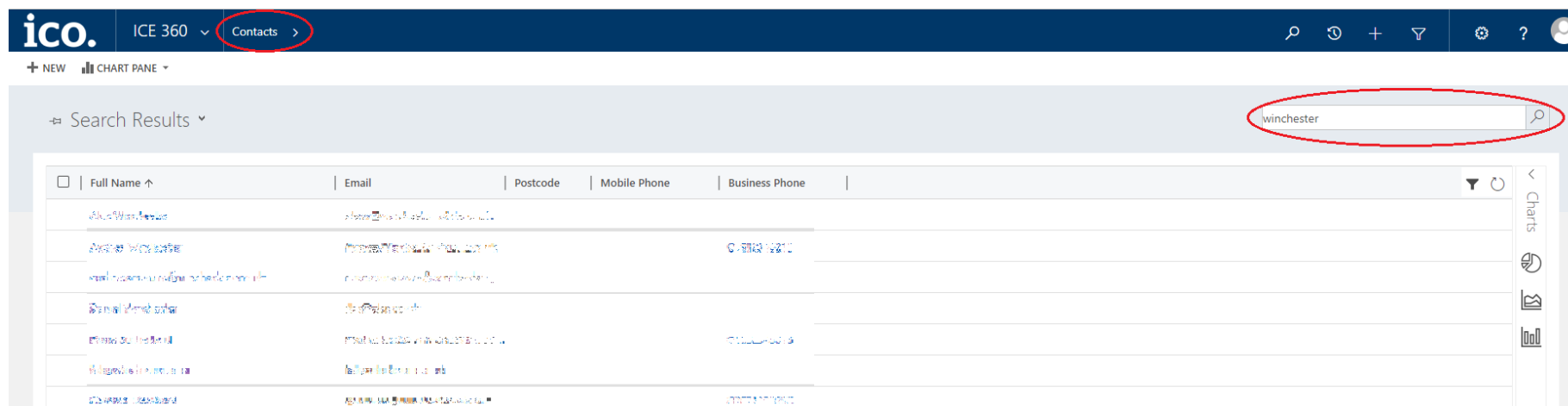
4. As this search function searches smaller sections of ICE 360 it is much quicker.

5. Ensure you are in the correct area of ICE 360 when using the local search function; otherwise it may appear there are no relevant records. For example, if you search for a name but you are in the 'Cases' area, you will get no results. This does not mean that your search term does not appear in ICE 360, just not in the section you are in.
6. In 'Contacts' you can search under name, email, telephone number or postcode (not postal address).
7. In 'Accounts' you can search under organisation name or postcode.
8. In 'Cases' you can search for all or part of a case reference.
9. In 'Activities' you can search for anything that appears in an email subject line, or a case reference.

Other resources: ██████████████████████████████   ICE 360 manual.

Section updated: 19 February 2024.

Filtering Information in ICE 360

Task

Filtering information in lists in ICE 360 to remove unwanted data or to narrow search results. You can use this to find specific types of cases by summary, outcome, date etc.

Steps

1. Any list (or 'system view') in ICE 360 can be filtered.
2. The global filter function in the blue ribbon is not in operation. Use the local filter function below it.
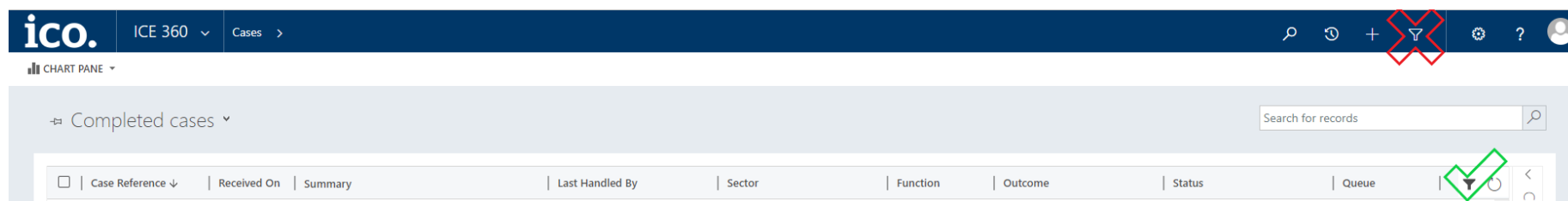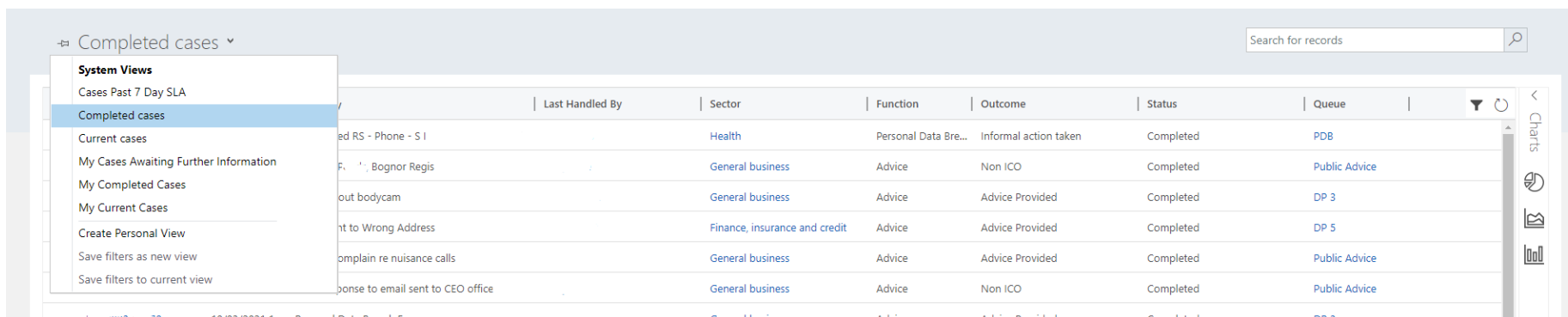
3. A black filter icon indicates filtering is switched off.
4. An outline of the filter icon indicates filtering is switched on. There will also be drop down arrows at the top of each column to indicate those columns can be filtered.
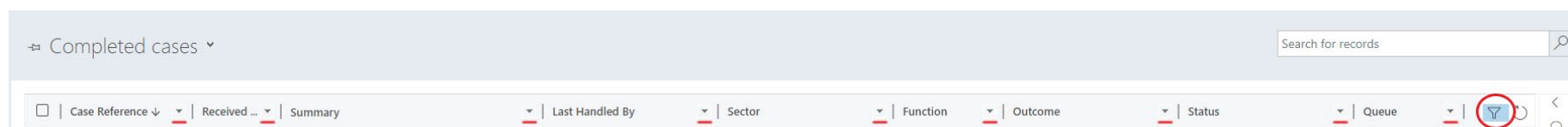
5. Columns can be quickly ordered by date or alphabetically by clicking the column header.
6. More detailed filtering can be done by clicking the drop-down arrow which opens a filtering menu. Each column has a different filtering drop down menu depending on the information listed in that column.

Example

1. You may have been allocated a FOI request for information about [Organisation Name] data breaches, and you want to view previous similar request cases.
2. The following example explains how to filter cases down to completed Information Rights cases, where the case summary mentions '[Organisation Names]' and 'PDB'.
   a. Go to Cases > Completed cases. You could also choose 'Current cases' if you are interested in open cases, or 'My Completed Cases' or 'My Current Cases' if you want to filter your own cases.

   b. Switch on filtering by clicking filter icon > open the filtering drop down menu for the 'Function' column by clicking the drop-down arrow > select the 'Information Rights' checkbox > click ok.

The completed cases list will now show only Information Rights cases.

c. Open the filtering drop down menu for the 'Summary' column > select 'Custom Filter'.

A pop out box titled 'Custom Filters' will appear.

d. Enter the required search terms to include or exclude. In this case we want to search for case summaries that contain '[Organisation Name]' *and* 'PDB'. Then click OK.
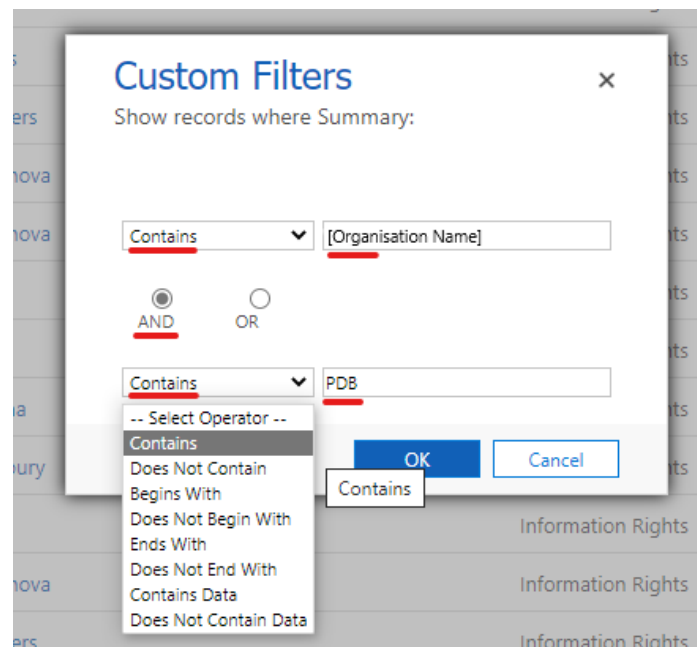
e. The results list will show all Information Rights cases where the summary features the terms '[Organisation Name]' and 'PDB'. The list could be further filtered by case outcome, case status, date request was received, name of IA Officer etc.

3. Note that searching case summaries is not fool proof for finding a certain type of request. It will depend on the level of detail and consistency of terms used in the case summary.

Section updated: 21 February 2023.

Searching CMEH Legacy

Task

Search CMEH Legacy for cases and parties formerly held on the CMEH case management system.

Steps

1. To access CMEH Legacy go to ███████████ CMEH Legacy.
2. At the top of this page, you should see a number of links, including:

CMEH Legacy Home Page   Search for a Case   Parties List

3. To search through cases on CMEH Legacy, click 'Search for a Case'.
4. Enter the case reference you are searching for in the 'Title' field, then click 'search'.

Title: RFA00000001
Content Type:
Party: ○
File: ○
Case: ◉
search

5. If the case is still held on CMEH Legacy, it will appear below. Click the link to access the case.
6. To search for an individual or organisation (a 'party'), click 'Parties List'.
7. Enter a term in the 'Find an item' field. Be specific, and consider any likely variations to the party name.
8. You can search for organisation or complainant name, email addresses and/or postal addresses.
9. Search results are displayed as a list of cases relevant to the party searched. The case reference numbers are not hyperlinked to the individual cases, so will need to be searched separately to access the file.

Section updated: 21 December 2022.

Creating Snapshots in ICE 360

Task

Create snapshots of cases on ICE 360 to create a single PDF of the documents and correspondence on a case.

Steps

1. Open the case in ICE 360 and go to Case: Documents.
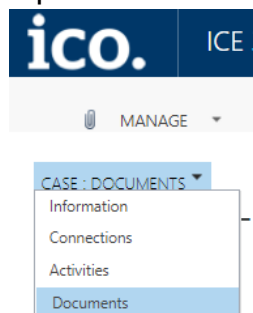
2. Above the list of documents there are several grey buttons. Select the 'Snapshot' button.

3. A dialogue box will appear. If you want to create a snapshot of only the case documents, select 'OK'. To include case activities (emails) in the snapshot, tick the 'Include Activities' checkbox then Click 'OK.'
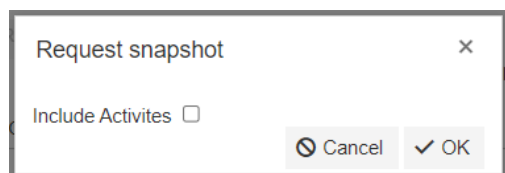
4. ICE 360 will now generate a new document on the case titled 'Snapshot_XXXXXX_XXX.pdf.'

	DISPLAY NAME ⬍	CATEGORY ⬍	LABEL ⬍	CREATED ON ⬍	STATUS ⬍	
☐	Snapshot_24012022_1153.pdf	Case snapshot	Case Rendition	24/01/2022 11:53	Pending	✎ Edit

5. Initially the snapshot status will say 'Pending.' The time it takes to generate a snapshot will vary based on the size of the case file. There could be a delay of several minutes.

6. To check if a snapshot is ready, refresh the page by pressing F5 on your keyboard, or by clicking on the refresh button at the top of your browser.

7. When a snapshot has been successfully generated, the status will change to 'Ready' and the title will appear as a blue hyperlink.

DISPLAY NAME ⬍	CATEGORY ⬍	LABEL ⬍	CREATED ON ⬍	STATUS ⬍
Snapshot_24012022_1153.pdf	Case snapshot	Case Rendition	24/01/2022 11:53	Ready

8. In some cases, ICE 360 may not be able to generate a snapshot and the status will show as 'Error'. If this happens, contact IT Help.

	DISPLAY NAME	CATEGORY	LABEL	CREATED ON	STATUS
☐	Snapshot_23032021_1139.pdf	Case snapshot	Case Rendition	23/03/2021 11:39	Error

9. Snapshots are automatically deleted from ICE 360 after 24 hours. This means that if you do not download and save the snapshot within this time, you will need to create a new one.

Key contacts: IT Help.

Section updated: 10 November 2022.

Checking Snapshots

Task

Check that a snapshot has included all the documents and activities from a case.

Steps

1. The first page of every snapshot is a coversheet that lists the Included and Excluded Documents and Activities. In ICE 360, 'Activity' refers to an email or webform.
2. Check if any documents or activities are listed as 'Excluded.'
3. Any excluded documents or activities will need to be downloaded from the case manually and added to the PDF in Adobe. See later section on how to download individual emails and documents from ICE 360, and how to add pages to a PDF.
4. If an activity includes attachments, the snapshot will produce an Email Attachment Coversheet.
5. Check each Email Attachment Coversheet for included and excluded documents, as above.
6. Snapshots will generally include all .docx and PDF documents but has difficulty generating .eml attachments.
7. Any excluded attachments will need to be manually downloaded and added to the PDF, as above.
8. Coversheets do not need to be provided to requesters as part of an information disclosure.

Section updated: 24 November 2022.

Download Individual Emails and Documents From ICE 360

Task

To download an individual email or document from ICE 360, rather than downloading a snapshot.

Emails

1. Open the email from the 'Case: Activities' area of the case in ICE 360.
2. Click on the cog icon in the blue bar at the top right of the screen.
3. Click Print Preview from the drop down menu.
4. Click the Print button in the top left of the pop out menu.
5. Select 'Save As PDF' in the Printer drop down, then click Save.
6. Choose where you want to save the document, then click Save.

Documents

1. Open the document from the 'Case: Documents' area of the case in ICE 360.
2. If it is a PDF, the document will open in a new browser tab.
   a. Click the save icon in the top right corner of the browser window.
   b. Choose where you want to save the document, then click Save.
3. If it is another type of document eg Word, it will open the document in the relevant programme.
   a. Go to File > Save As.
   b. Choose where you want to save the document, then click Save.

Section updated: 20 June 2023.

Applying Extensions

Background

In certain circumstances, the statutory deadline for SARs and FOI requests can be extended. The timeframe for a SAR can be extended for an additional two months if the request is deemed to be 'complex' (unless it is a DPA 2018 Part 3 SAR which must be responded to within one month). With regards to the FOIA, the timeframe can be extended in certain circumstances where a qualified exemption is engaged, and additional time is required to consider the public interest test.

Task

Apply extensions to statutory timeframes for information requests.

Extending SAR timeframes

1. Once you have identified the information in scope of the request, consult ICO guidance on when a request can be considered complex.
2. If you are considering extending the timeframe, speak to your line manager and document the decision in a case note.
3. You will have an additional two months to respond to the SAR. Change the due date in the case summary, and the metadata in 'Case: Activities' > Case Activities tab > click case reference hyperlink.
4. Inform the requester of the extension within the original deadline. Explain the reason for the extension and provide the new due date. You do not need to go into detail but ensure that you provide adequate reasons, referring to our website guidance.

FOI requests – Public Interest Test (PIT) extensions

1. Identify whether a qualified exemption (such as section 31) applies to any of the information in scope of the request. The exemption needs to be engaged, and you need to have completed the prejudice test and determined that disclosure would prejudice a relevant function.

2. Determine whether more time is needed to consider the PIT in respect of the relevant information. You should consult the [ICO detailed guidance on the PIT](#).

3. If you have reached the conclusion that more time is needed, then the 'public interest extension' will apply. The extension is defined as a 'reasonable' time in the legislation, whereas our guidance states that it should not take more than an additional 20 working days to consider the PIT, and in any case should be completed as soon as is possible.

4. The PIT extension only covers the information to which the qualified exemption applies. Our guidance states that any information in scope which is either not exempt or is covered by an exemption which is not qualified will either need to be disclosed, or withheld and a refusal notice provided, within the original request deadline.

5. To make use of a PIT extension, you will need to write a response to the requester within the initial timeframe, using ███████████████████████████████ PIT Extension Generic.

6. Change the metadata on the ICE 360 case to reflect the new timeframe. 'Case: Activities' > Case Activities tab > click case reference hyperlink.

Other resources: ICO website - [Guide to managing an FOI request | ICO](#).

        ICO website - [Right of access | ICO](#).

Section updated: 8 February 2023.

Internal and External Consultation

Task

A consult may be internal with a colleague or external with a data controller or public authority. An appropriate colleague can assist with understanding if and where information is held and provide views on disclosure. We should also consider external views on the disclosure of information we hold.

Internal consultation
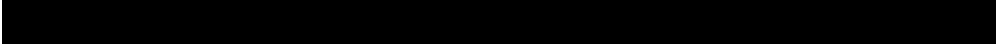
1. Read the request and identify the business area or areas where information might be held.
2. Review ████████████████████████████████████ Team contacts for requests to ICO and identify the appropriate contact.
3. If struggling to identify a contact, take the request to Request Queries.
4. Send the consult email in Outlook using the internal consultation template (███████████████████ ███████████████████████████████). Copy in icocasework@ico.co.uk and include the request case reference in the subject line so it attaches to the case in ICE 360.
5. The purpose of the email and the case reference number should be clear in the subject line.
6. Allow five working days for a response to a consultation. Include 'please respond by' date in the email.

It is important to send key communications about a case in Outlook to the case in ICE 360 for completeness of the case record.

External consultation

1. Review the request, identify the parties involved.
2. If the request relates to a complaint case, check the ICE 360 complaint 'Case: Connections' which should include a 'Submitted About Party' and 'Account Contact' role.
3. An organisation's mailbox for information rights matters would be the preferred contact point because it will be regularly monitored. Alternatively the 'Account Contact' and/or DPO could be consulted.

4. Add the account and contact for external consultation to your case by following the instructions in ██████████████████████████████████ ICE 360 case handling procedure ('Progressing the case - DC consultations' see page 14).
5. Prepare an external consult using the appropriate template:
    a. Consultation with data controller template - SAR or Hybrid, or
    b. Consultation with external body template - FOI.
6. PDF the information in scope of the consultation and upload it to the 'Case: Documents' section of the information case. This will allow you to attach it to the consultation email.

Section updated: 22 November 2022.

Information Classification

Task

To classify and protect information according to its value to the organisation by complying with the UK Government Security Classification Policy.

All information falls into one of three levels of classification to indicate its sensitivity: OFFICIAL, SECRET and TOP SECRET. We can also apply the information classification sub-set OFFICIAL SENSITIVE.

Steps

1. Treat information about routine business operations and services as OFFICIAL. Note – the vast majority of the information we handle in IA with be OFFICIAL.
2. Do not security mark routine OFFICIAL information.
3. Treat information that could have more damaging consequences if lost, stolen or published as OFFICIAL SENSITIVE.
4. A decision to classify information as OFFICIAL SENSITIVE can be taken by IA on a case-by-case basis.
5. Mark OFFICIAL SENSITIVE information with that classification at the top of each page.
6. Include the OFFICIAL SENSITIVE classification in the subject line of all relevant emails.
7. Mark information with the highest level of classification applicable. For example, a mixed information bundle of SECRET and OFFICIAL SENSITIVE, must be marked as SECRET.

Other resources: Iris - Information Classification Guidance.

                    External website - Government Security Classifications - gov.uk.

Key contacts: Iris - Cyber Security Services.

Section updated: 10 May 2023.

Writing a Response

Task

Writing a response to an information request, ensuring it meets the statutory requirements and that all formatting and content is consistent and appropriate.

Steps

1. Use IA response templates as the basis for your response letter or email (███████████ ████████), but adapt them as appropriate.
2. Use headed letter templates to ensure your response includes the ICO logo and contact details.
3. Use Verdana 12 for the body of the text, unless the requester has a reasonable adjustment for another font/size.
4. Respond via email from ICE 360 unless the requester has asked for a postal response and it is reasonable to comply with this request.
5. Any attachments to an email must be sent as a PDF file, or .csv file if sending a dataset. An outgoing email plus its attachments cannot exceed 15MB when being sent from ICE 360.
6. Unless otherwise indicated, your response should include the following:
   a. Your name, job title and direct contact details. However, you can use discretion. If you have concerns about disclosing these details under certain circumstances, consult your manager.
   b. For SARs, confirmation whether we are processing personal data about the requester.
   c. For FOI requests, confirmation whether we hold the requested information (unless issuing a 'neither confirm nor deny' response, a vexatious refusal, or where confirming if the information is held would exceed the cost limit).
   d. A broad explanation of what information is being withheld (if applicable and appropriate) and the specific legislation that has been applied.

e. For FOI requests, advice and assistance where appropriate, as per section 16 FOIA. See Section 16 – Advice and Assistance for guidance on when to do this.

f. For EIR requests, ensure you provide advice and assistance where appropriate, as per regulation 9 EIR. See Regulation 9 – Advice and Assistance for guidance on when to do this.

g. Information on what to do if the requester is unhappy with our response. They should first seek clarification from IA, but if they remain dissatisfied they can ask for an Internal Review (FOI and EIR requests only) or make a complaint to the regulatory arm of ICO via the Data protection and personal information complaints tool. Requesters can also make a complaint if they are unhappy with the service we have provided.

Section updated: 19 February 2024.

Closing a Case

Task

Closing an information request case in ICE 360.

Steps

1. Once a request response has been sent, add appropriate display names to all 'Case: Activities' correspondence and 'Documents' on the case. Ensure that withheld information is clearly labelled.
2. Add a case note if necessary. Outline your approach, considerations regarding any exemptions applied etc. This can be added as a document, or by emailing your case note to the case.
3. Save all changes at each step or the changes will be lost.
4. From 'Case: Activities', select the Case Activities tab. Click the hyperlinked case reference number to open the information request activity page.
5. Populate the date response sent field. If the response is late, supply a late response reason from the dropdown. It is important to complete these fields for our performance statistics.
6. If information has been withheld, select Withheld Reasons in the grey banner and select all exemptions that have been applied to withhold information.
7. Check that all emails and other activities have been 'completed'. This will ensure they are removed from your ICE 360 inbox (on the home screen). To complete an email, open it, select 'Complete', and 'Do not mark as secondary'. Only select 'Mark as secondary' if the item was secondary correspondence ie follow up queries or complaints.
8. Complete the case by clicking Action on the grey ribbon, then click Complete.
9. A list of information management reminders will appear. Check you have done these, then click Confirm.

10. If you have not done so already, you will now be able to input details including the closure channel, outcome etc. in the 'Complete case' screen.

    a. Click Yes for 'Proactive disclosure' if you are adding an FOI response to the ICO Disclosure Log. If you are not adding an FOI response to the Disclosure Log, ensure you add a case note to the case to explain why.

    b. Click Yes for 'Preserved' if the case needs to saved beyond the typical retention period.

Complete case

Closure channel:	○ Email ○ Phone ○ Letter
Proactive disclosure:	○ Yes ◉ No
Preserved:	○ Yes ◉ No
Legislation Reasons	Art 15 - Right of access
	Legislation reasons...
Category of request	DP concerns
	Category of request...
	Outcome...
	Withheld reasons...

11. Check the case events on the 'Case: Information' page to see that the outcome has been logged and that the case status has changed to from 'In Progress' to 'Completed'. A completed case should no longer appear in your work queue on your ICE 360 dashboard.

Other resources: ███████████████████████ IA ICE 360 case handling procedure.

Section updated: 30 January 2024.

Withholding Information

Introduction

Transparency is a key principle in data protection. The FOIA and other information legislation also provides an opportunity for public authorities, including the ICO, to develop relationships with the public based on openness and transparency. However, there will be times when information cannot or should not be disclosed.

This section highlights some of the key circumstances in which the ICO might need to withhold information or refuse a request, including the exemptions we most frequently apply, and how these should be conveyed to requesters in our responses.

Refusing a Request

Task

To understand and correctly apply the legislation when refusing an information request where appropriate.

Remember: every request must be considered individually and on its own merits (unless you believe it is a repeat request), and if you refuse a request you must clearly explain why to the requester.

UK GDPR Article 12(5) – Manifestly Unfounded or Excessive

1. It may be appropriate to refuse a SAR if you can demonstrate that the intent is to cause disruption or harassment, rather than being a genuine request to access personal data.
2. Examples: a requester makes a SAR but suggests they will withdraw it in return for something; a repeat request for specific personal data immediately following a previous identical request.
3. See ICO website - When can we refuse to comply with a request? - GDPR
4. You can decide to respond to a request of this nature and include a warning to the requester in your response. You can consider if an individual has received a previous warning, but be aware that a previous warning on its own is not sufficient grounds to refuse a request.

FOIA Section 12 – Cost of Compliance Exceeds Limit

1. You may be able to refuse a request if the cost of determining if you hold the information, and finding, retrieving and extracting the information, would exceed £450 (equivalent to 18 hours of work).
2. Examples: a request for all information held by ICO on a very broad topic where this could include internal emails, Teams chats, case notes etc; a request for details of all DP complaints to the ICO that mention SARs involving CCTV.
3. The entire request can be refused under section 12 even if just one part would engage section 12. However, this does not apply if there are different parts of the request that are unrelated.

4. When calculating costs, requests can be aggregated if the requests are from the same person, or a group acting together, received within a 60 working day period, and ask for the same, or similar, information.
5. Explain to the requester how you calculated the cost. See ICO guidance about what to do when the [costs of compliance exceed the appropriate limit](#).
6. There is no requirement for you to carry out a public interest test when engaging section 12.
7. If engaging section 12 you must provide advice and assistance as to how the request could be narrowed or rephrased in a way that section 12 would no longer apply.

FOIA Section 14 – Vexatious / Repeated Requests, Grossly Oppressive Burden

1. You may be able to refuse a request if you can demonstrate that the request is vexatious, or responding would cause a grossly oppressive burden to the organisation.
2. The entire request can be refused under section 14 even if just one part would engage section 14. However, this does not apply if there are different parts of the request that are unrelated.
3. There is no requirement for you to carry out a public interest test or to confirm or deny whether you hold the requested information when engaging section 14.
4. You can decide to respond to a request of this nature and include a section 14 warning to the requester in your response. You can consider if an individual has received a previous warning, but be aware that a previous warning on its own is not sufficient grounds to refuse a request.
5. If you refuse a request under section 14, you may want to include a [section 17(6)](#) warning, advising that future requests on the same subject may be refused and not receive a response.

Vexatious or Repeated Requests

1. Examples: "provide me a summary of all your cases that demonstrate your utter incompetence and corruption"; several requests for an investigation outcome in a short space of time when the requester has been advised the investigation is ongoing.
2. See ICO website - [Dealing with vexatious requests (section 14)](#).

Grossly Oppressive Burden

1. Examples: a request for a substantial volume of disclosable information but where significant quantities of exempt information are scattered throughout.
2. See ICO website - How do we deal with a single burdensome request?

Other resources: ███████████████████████████ for templates

██

████████████ Withheld Reason Summary to find previous examples of refused requests.

External websites - UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000.

Section updated: 19 February 2024.

Applying Exemptions – SARs

Task

To understand and correctly apply the legislation when exempting (withholding) information where appropriate in a SAR response.

Remember: every request must be considered individually, and if you withhold information you must clearly explain why to the requester.

Also remember that anything that is not the requester's personal data can be redacted or withheld without the need to apply an exemption as it is out of scope.

The following are exemptions commonly used by the ICO under DPA 2018, but other exemptions may apply. See A guide to the data protection exemptions for more detailed guidance.

DPA 2018, Schedule 2, Part 3, Paragraph 16 – Third Party Personal Data

1. This exemption might apply to information that is the personal data of a third party.
2. Examples: a response to a DP complaint that includes the names and opinions of employees at the data controller; the direct contact details of third parties.
3. See ICO website - What should we do if the request involves information about other individuals?.

DPA 2018, Schedule 2, Part 2, Paragraph 11 – Regulatory Function of the Commissioner

1. This exemption might apply to personal data of the requester that, if disclosed, could prejudice our ability to perform our regulatory functions.
2. Examples: personal data regarding the requester contained within documents relating to an ongoing complaint, investigation or audit; correspondence from a data controller/public authority explaining their position regarding a complaint to ICO.
3. See ICO website - Exemptions | ICO.

DPA 2018, Part 5, Section 132 – Confidentiality of Information

1. This exemption might apply to information provided to the ICO by an organisation in the course of carrying out our regulatory functions, and the information relates to an identifiable business or individual, and is not already publicly available.
2. **It is a criminal offence to disclose such information without lawful authority**.
3. Examples: any information provided to the ICO in confidence, such as correspondence from a data controller/public authority explaining their position regarding a complaint to ICO; an internal document provided by a business that is not available elsewhere.
4. Rather than automatically exempting such information, it is good practice to seek views on disclosure from the provider of the information unless they have already indicated whether the information should be treated in confidence.

Other resources: ███████████████████████████ for templates.

External websites - UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000.

Section updated: 17 April 2023.

Applying Exemptions – FOI Requests

Task

To understand and correctly apply the legislation when exempting (withholding) information where appropriate.

Consider every request individually. If you withhold information you must clearly explain why to the requester. Also consider the duty to confirm or deny (this may not apply if certain exemptions are engaged), and the Public Interest Test (PIT) which will apply when engaging a qualified exemption.

The following are exemptions commonly used by the ICO, but other exemptions may apply. See Freedom of Information Exemptions and When can we refuse a request for information? for more detailed guidance.

FOIA Section 21 – Information Accessible By Other Means

1. This exemption might apply when a request is made for information already reasonably available, such as on the ICO website, or on the UK Government Web Archive.
2. Examples: information already on the ICO Disclosure Log; statistics already available in the Complaints and concerns data sets; information otherwise already published on the ICO website.
3. PIT not required to engage this exemption.
4. No option for a 'neither confirm nor deny' (NCND) response if applying this exemption.

FOIA Section 22 – Information Intended for Future Publication

1. This exemption might apply to information that exists and is intended to be published in future. The exact intended date of publication does not have to be fixed. If the publication date is not fixed you should provide the requester with an estimated date of publication where possible.
2. Examples: information regarding expenditure due to be published next month in our Annual reports; a dataset due to be published in the next round of pro-actively published datasets.

FOIA Section 31 – Law Enforcement

1. This exemption might apply to information that, if disclosed, would or would be likely to prejudice our ability to regulate the laws we oversee.
2. Examples: information about an ongoing PDB investigation, or audit, or other situation where we are deciding whether to take regulatory action; a request for ICO internal email addresses.

FOIA Section 36 – Prejudice to Effective Conduct of Public Affairs

1. This exemption might apply to information that, if disclosed, would or would be likely to prejudice the effective conduct of public affairs.
2. Examples: information held about ICO discussions with UK government on live matters of policy development; ongoing consultations regarding the development of UK-wide data-sharing projects.
3. See Section 36 - Prejudice to the effective conduct of public affairs for ICO guidance, and the 'Section 36' guidance in the following section.
4. When considering this exemption you must discuss it with your line manager. IA must also seek the opinion of the 'Qualified Person'; in our case that is the Information Commissioner.

FOIA Section 40(2) – Personal Information of Third Parties

1. This exemption might apply to information that is the personal data of a third party.
2. Examples: information about who has complained about the use of the requester's domestic CCTV system; detailed information about ICO employees such as their qualifications or their special category data.
3. PIT not required to engage this exemption.

FOIA Section 42 – Legal Professional Privilege (LPP)

1. This exemption might apply to information that has been shared between a client and their professional legal adviser relating to advice or ongoing legal action.
2. Example: internal ICO legal team discussions on adopting a policy position, or developing official guidance on matters of information law.

FOIA Section 44 / DPA Section 132 – Prohibitions on Disclosure

1. This exemption might apply to information that engages a prohibition applicable in any other law. Disclosure of information provided to the ICO by an individual or organisation and for which we do not have lawful authority for disclosure is prohibited under DPA section 132.
2. The exemption in DPA section 132 might apply to information provided to the ICO by an organisation in the course of carrying out our regulatory functions, and the information relates to an identifiable business or individual, and is not already publicly available.
3. **It is a criminal offence to disclose such information without lawful authority.**
4. Examples: any information provided to the ICO in confidence, such as correspondence from a data controller/public authority explaining their position regarding a complaint to ICO; an internal document provided by a business that is not publicly available elsewhere.
5. PIT not required to engage this exemption.
6. Rather than automatically exempting such information, it is good practice to seek views on disclosure from the provider of the information unless they have already indicated whether the information should be treated in confidence.

Other resources: ██████████████████████████ for templates.

ICO website - Freedom of Information Exemptions.

External websites - UK GDPR, Data Protection Act 2018, Freedom of Information Act 2000.

Section updated: 17 April 2023.

Section 36

Task

Obtaining the Qualified Person's opinion when applying section 36 of the FOIA.

Steps

1. If you are handling a request and believe that section 36 ([Section 36 - Prejudice to the effective conduct of public affairs](#)) may be engaged, contact your manager to discuss.
2. Once you have spoken with your manager, if section 36 is still being considered as an exemption, your manager will send a covering email to the Head of Department and Director for their agreement.
3. If the Head of Department and Director agree that the request should progress to the Commissioner for a decision, your manager will do this via the Commissioner's Private Office in time for either the Commissioner's Tuesday or Thursday box.
4. The Commissioner requires that the Qualified Person template (████████████████████████████ ███████████████████████ Template for recording opinion of qualified person (section 36)) is attached to the email along with the exempt information which should clearly outline the proposed redactions.
5. If the Commissioner agrees to the exemption, you will receive notification from his Private Office. You can then issue the response.
6. Note that a PIT extension, if needed, can only be applied once the Commissioner agrees section 36 is engaged.
7. Please ensure that requests are considered promptly upon allocation to ensure that there is enough time within the statutory deadline to allow for the request to be put into one of the twice weekly Commissioner boxes and for the Commissioner to consider his opinion on whether to disclose the information in scope.

Section updated: 5 May 2023.

ICO Staff Information

Task

Consider if ICO staff information is suitable for disclosure.

Steps

1. Before disclosing any information, check if any ICO staff information is included.
2. Information should be considered on a case-by-case basis, but it is reasonable to disclose some information about staff in certain roles. Decisions should be made with reference to the ICO Employee information disclosure policy.
3. It is usually reasonable to disclose some information about public facing staff, such as case officers, and executive team members.
4. People Services maintain a list of ICO staff whose personal circumstances mean that their information should **not** be disclosed. Ensure you check this list each time when considering a disclosure of staff information, or consult with the staff members themselves.
5. More detail on what information is likely to be appropriate to disclose is listed in the policy linked below.
6. Staff mobile telephone numbers should not be disclosed.

Other resources: ICO Website - Employee Information Disclosure Policy.

Section updated: 19 February 2024.

ICO Internal Email Addresses

Documents in scope of requests may sometimes include internal ICO email addresses, such as emails for specific internal teams. To prevent misuse, these emails addresses must not be disclosed.

Task

Use the appropriate exemption to withhold internal email addresses.

Steps

1. Check in scope documents for internal email addresses. A non-exhaustive list can be found on the internal email exemption template. The most commonly occurring are the emails for IT, PADPCS groups, and for publishing decision notices.
2. For SARs, internal email addresses can be considered out of scope of the request and so should be white-redacted and labelled 'out of scope'.
3. For FOI requests, internal email addresses can be withheld under section 31. This requires a public interest test. An example of a PIT can be found on the internal email exemption template.

Section updated: 24 January 2023.

Other Types of Requests

Introduction

Most requests we receive are for personal data relating to a complaint case, or for information about the work and operation of the ICO. More often than not these requests are submitted by email.

This section explains how to handle those requests that require an alteration to our standard procedure. Our approach may also need to differ when requests require more sensitive handling.

High Profile FOI/EIR Request Alert Procedure

Background

The IA Team frequently respond to Freedom of Information and EIR requests that are potentially high profile in nature. By this, we mean that our response may garner media attention or comment from stakeholders, bloggers, journalists etc. To ensure that appropriate ICO staff are made aware that such requests have been received by the organisation, and to appraise them of our response before it is sent outside of the ICO, IA staff are required to use the following procedure. This never applies to SARs.

Task

Handling Freedom of Information and EIR requests considered to be potentially high profile.

Steps

1. Establish that a request is potentially high profile. Criteria to consider:
   - Requests following high profile media coverage of issues that the ICO might already be addressing.
   - Requests relating to ICO strategic files/high profile investigations.
   - Requests made by journalists or bloggers.
   - Requests about ICO corporate issues or internal compliance, particularly about internal compliance with UK GDPR/FOIA.
   - This list is not exhaustive. There may be other requests that do not match these criteria but that should be deemed potentially high profile. If you are unsure whether to treat a request as potentially high profile, please consult an IA Manager.
2. Once a request has been deemed potentially high profile, IA Officer should send out request alert emails as soon as possible.
3. The first email should go to ████████████████████████████████, cc'd to IA Managers.
   a. Use the HP Request Alert Email - Commissioner Group Only template.

     b. Ensure that 'Potentially High Profile Request' is in the subject line with a short description of the request.

     c. This email should include the name of the requester, unless they are a protected person or whistle-blower*.

4. The second email should be sent to ██████████████████, cc'd to IA Managers.

     a. Use the HP Request Alert Email template.

     b. This email should **not** include the name of the requester.

     c. This group includes a number of staff throughout the organisation who will likely have an interest in knowing that a potentially high profile request has been made. They may be able to offer information as part of a consult or need to be aware that a particular response is due to be sent out for their own engagement purposes. This group does not need to know who has made the request and therefore the name of the requester does not need to be included.

5. Carry out all of the required steps in order to respond to the information request, ie collate information, consult and draft a response.

6. Send out Request Alert emails at the end of the process with the proposed response and any disclosures (if applicable).

7. Again the first email should be sent to ████████████████████████████████, cc'd to IA Managers.

     a. This email should include the name of the requester, unless they are a protected person or whistle-blower*.

8. The second email should be sent to █████████████████, cc'd to IA Managers.

     a. This email should **not** include the name of the requester for the same reasons outlined earlier in the procedure.

9. Allow appropriate time for staff receiving the Request Alert emails to make comments (eg 24 hours). However, bear in mind that once a response is due to be sent out, all of the necessary consultations should have already taken place. IA Officers should clearly state when they intend to issue the response and the date it is due. The Request Alert emails are a way of informing staff of what we intend to put into the public domain, and comments should only be made if they are relevant and necessary.

10. If comments are received from the Request Alert group, IA Officers should consider these as appropriate and amend the response if required.
11. Send the response to the requester.
12. Ensure Request Alert emails are saved onto the case file in ICE 360.

*Why are we including the requesters name when the FOIA is applicant blind?

We are including the name of the requester in this instance as it is necessary for the Commissioner, his Private Office and a limited number of Communications staff to be privy to this information. This is because the Commissioner should be fully aware of the types of requests that are being received by his office and from whom, in the event he is asked about a request in the course of his engagements. Similarly it is necessary for some senior Communications staff to have this information due to their role in monitoring the ICO's social media accounts and responding to queries received this way.

How are we able to do this?

Requesters are aware that their names and contact details will be used as part of the processing of their request. This is outlined in our Privacy Notice. Requesters names are not confidential and appear on ICE 360. The majority of IA casework is not restricted and is therefore viewable by most ICO staff.

Information requests can be received by anyone at the ICO. Requests are frequently made on the back of DP or FOI complaints and forwarded to IA by Case Officers. In these instances, staff outside of IA are aware of the request having been made and will potentially be involved in the consultation process.

Finally, the Information Commissioner is a corporation sole – all of the ICO activity is done on behalf of the Commissioner via delegated authority. In this sense it is completely practical that the Commissioner should be aware of who is making requests to him and what is being sent out and to whom on his behalf.

Whilst we have a legitimate purpose for sharing the name of a requester with a small number of staff, the principle that the FOIA is applicant and motive blind remains. High profile requests are not handled differently —

for example, handled more quickly, or involving the disclosure of more or less information — because a requester's name has been shared.

However, there are a small number of circumstances when it will not be appropriate to share the name of the requester with the Commissioner or any staff outside of IA. In the case of protected persons or whistleblowing the name of the requester should not be featured on either Request Alert email. If you are dealing with a protected person or whistle-blower, please consult an IA Manager before sending a Request Alert email.

Other resources: ICO website - Whistle-blowing Policy.

Key contacts: IA Group Managers.

Section updated: 18 November 2022.

WhatDoTheyKnow (WDTK)

Whatdotheyknow.com (WDTK) is a website that can be used by individuals to make FOI requests. Requesters post requests onto the website, which then submits the request to the relevant Public Authority (PA). When the PA sends a response it is automatically published on the WDTK site. Each request made on WDTK generates a unique email address, even if the requester has used the site before. All correspondence between requesters and public authorities carried out via WDTK is published on the website.

Task

Handling information requests via WDTK.

Handling requests

1. We only handle FOI requests via WDTK, we do not respond to SARs, enquiries or other data rights requests in this way. If we receive a SAR via WDTK, a response must be sent to the requester advising them it will not be progressed via this channel and providing them with details of how to contact the ICO directly in order to make their request.
2. As WDTK is a public website, if you ask for clarification and/or when you send a response, you can remove your name and direct dial from correspondence.
3. Send the response to the requester at the single-use email created by WDTK for each request, unless the response is unsuitable for a public forum such as WDTK.

Section 14

IA Officers should exercise caution when responding to requests made via WDTK that engage section 14. Each request should be addressed on a case-by-case basis. However, there are some universal approaches that can be followed when section 14 is engaged due to grossly oppressive burden or a repeated request. If an IA Officer needs to provide detail about the requesters conduct to justify a vexatious response, this should be done away

from WDTK in direct communication with the requester in order not to publicly disclose any of their personal data. IA Officers can still state that the request is being refused under section 14 on WDTK in order to meet the requirements of the FOIA, but must advise the requester to provide a personal email address or other means of contact in order to establish the details behind the refusal.

Section 50

The ICO does not accept requests for section 50 complaints via WDTK due to the amount of personal data our response would entail. If a requester submits a section 50 complaint via WDTK, recommend that the requester contact the ICO directly using their personal email or other means of direct contact. Ensure you provide the complainant with ICO contact information in order to do this.

Personal data requests and complaints

Because all responses to WDTK requests are published online, the ICO does not accept any requests under UK GDPR via WDTK. If you receive a SAR, request for rectification or erasure, or any other request related to personal data, provide information regarding how to contact the ICO directly to submit these requests.

If a requester shares their personal data via WDTK, please contact WDTK in order to alert them and ask for the post to be taken down. WDTK will contact the requester to let them know the post has been removed.

Similarly, data protection and FOI complaints are not accepted via WDTK. If an individual attempts to submit a complaint via WDTK, provide information regarding how to contact the ICO directly.

Other resources: ████████████████████████ for templates.

Section updated: 31 October 2022.

Requests on Domestic CCTV Complaint Cases

Background

The Court of Justice of the European Union (CJEU) issued its judgment in the case of Ryneš on 11 December 2014. In this judgment, the CJEU concluded that where a fixed surveillance camera faces outwards from a private domestic property and captures images of individuals beyond the boundaries of that property, particularly where it monitors a public space, the recording cannot be considered as being for a purely personal or household purpose. Therefore, in the UK the recording would become subject to the DPA.

A requester usually wants to know what information is held on a CCTV complaint case. Information provided to us by individuals in the course of them making or responding to complaints about domestic CCTV is generally considered to have been provided with an expectation of confidence.

The complaint is the personal information of the complainant. Their submission may also contain the personal information of other individuals, often in relation to the circumstances of the complaint. However, in most cases it will be unlikely that these other individuals will be entitled to the information. We are unlikely to be able to obtain consent and we owe the complainant a duty of confidentiality. In many cases this is likely to outweigh any third party right of access.

Any detail required by either party in order to respond to queries will be given to them during the complaint handling process. The 'data controller', the 'CCTV operator' and the 'complained about party' are interchangeable terms used to refer to the individual who uses the CCTV camera. The 'data subject', the 'complainant' or 'third parties' would refer to any individual filmed by the CCTV camera.

Task

To consider requests for information received on domestic CCTV complaint cases.

Steps

1. If the request is from the complainant asking to see what we have sent to the CCTV operator, refuse under the FOIA section 40(2). The complainant can be supplied with an anonymised template copy of the letter to the CCTV operator. This can be handled as normal course of business by the case officer working on the complaint.
2. If the request is from the CCTV operator asking to know who made the complaint and the details of that complaint, refuse under the FOIA section 40(2).
3. If a request from the complainant or the CCTV operator is for their own personal data from a CCTV complaint case, consider this as normal as a SAR.

Section updated: 25 November 2022.

Hybrid Requests

Task

To distinguish when request cases need to be considered under both the DPA and the FOIA, or when two separate cases need to be set up.

Steps

1. If you receive a request for a DP case file from the complainant, this should be treated as a SAR. Information that is not the personal data of the requester should be considered and provided on a discretionary basis unless otherwise exempted from disclosure. Make clear in your responses which information has been provided on a discretionary basis.
2. If you receive a request for two discrete pieces of information, one for PD and another for non-PD, eg a policy or procedure, then two separate request cases should be set up in ICE 360 – one under the DPA and one under the FOIA. These will ideally be allocated to the same officer for continuity and can be responded to in the same email or letter to the requester.
3. If a request is received asking for an FOI complaint file that contains non-PD of the complainant, this should be set up as a hybrid request.
4. The deadline for a hybrid request is the earlier of the two applicable statutory deadlines, the FOIA or the DPA (usually the FOIA deadline of 20 working days).

Other resources: ███████████████████████████   Hybrid request – response template.

Section updated: 28 November 2022.

Rectification Requests, UK GDPR Article 16

Task

Processing a request for rectification of personal data under Article 16 of the UK GDPR. These requests can be made by any identifiable individual, either verbally or in writing.

Steps

1. Requests for rectification cases will be created in ICE 360 by an IASO.
2. Consider the request in line with the ICO guidance on the [right to rectification](#).
3. Personal data can be considered as inaccurate in matters of fact, or if the information is incomplete. Opinions are unlikely to be considered inaccurate.
   a. For example, if we have mis-spelt a requesters name in our records, the information is inaccurate and we would take action to correct this.
   b. However, if a requester disputes opinions expressed by a case officer in a call note regarding the tone of voice they used during a call, we are unlikely to take action on such a request.
4. Information is not considered inaccurate if it was correct at the time it was created.
   a. For example, a requester may change their name and ask us to change all historic documents that include their old name. We are unlikely to take action on such a request, but would use their new name in future.
5. Notify the requester of your decision using the GDPR Art 16 Response – Rectification template.
6. On completion, record the case outcome as appropriate. Unlike SARs or FOI requests, you can use the case outcomes 'Action taken', 'Partial action taken', or 'Refusal to take action' if appropriate.
7. If we refuse to take action, add a case note to all relevant cases on ICE 360. Explain that the data subject disputes the accuracy of the data, and specify what information they believe to be inaccurate and why.

Other resources: External website - UK GDPR Article 16.

External website - DPA 2018, Chapter 3, Rights of the data subject.

Section updated: 5 June 2023.

Erasure Requests, UK GDPR Article 17

Task

Processing a request for erasure of personal data under Article 17 of the UK GDPR. This is also known as the 'right to be forgotten'. These requests can be made by any identifiable individual, either verbally or in writing.

Steps

1. Requests for erasure cases will be created in ICE 360 by an IASO.
2. Consider the request in line with the ICO guidance on the right to erasure, and in line with our Retention and Disposal Policy in Policies and procedures on the ICO website.
3. A typical request for erasure might be for deletion of all personal data, or a particular case file. We are unlikely to do this if it conflicts with our retention schedule as this could prejudice our regulatory function.
   a. For example, a requester may be unhappy with the outcome of a complaint, and asks for the case file and their contact record to be deleted. We are unlikely to take action.
   b. However, a requester may have sent us identification in relation to a complaint and asks us to delete it once the case is complete. We are likely to take action if the ID is no longer required.
4. Notify the requester of your decision using the GDPR Art 17 Response - Erasure template.
5. If you agree to the request for erasure, consider that information for deletion may be held in ICE 360, SharePoint, and the Outlook files and desktops of case officers involved with the data subject.
6. To delete emails held in ICE 360 (in the Case: Activities area) you must contact IT Help. Prefix the email label in ICE 360 with 'DELETE', and provide as much information as possible to enable IT Help to identify the information to be deleted eg the case reference, email label, Activities page number, time and date.
7. To delete documents held in the Case: Documents area in ICE 360, tick the check box next to the relevant document, then click the grey 'Delete' button.
8. To delete an entire case, close the case with the Outcome of 'Mark for Deletion'. To delete an entire case that has already been closed, contact IT Help.

9. On completion, record the case outcome as appropriate. Unlike SARs or FOI requests, you can use the case outcomes 'Action taken', 'Partial action taken', or 'Refusal to take action' if appropriate.

Other resources: External website - UK GDPR Article 17.

External website - DPA 2018, Chapter 3, Rights of the data subject.

Section updated: 5 June 2023.

Restriction of Processing Requests, UK GDPR Article 18

Task

Handling a request for restriction of processing of personal data under Article 18 of the UK GDPR. These requests can be made by any identifiable individual, either verbally or in writing.

Steps

1. Requests for restriction of processing cases will be created in ICE 360 by an IASO.
2. Consider the request in line with the ICO guidance on the right to restrict processing.
3. We may consider restricting the processing of personal data if, for example, the accuracy of the data is disputed, or if a data subject asks us to hold data for longer than usual.
   a. For example, we may retain a case file beyond our retention period if the requester is involved in litigation to which the case file is relevant.
   b. Or we may cease contacting a requester if they ask us to, although this does not mean we would delete their cases or contact record.
4. Notify the requester of your decision using the GDPR Art 18 Response – Restriction template.
5. On completion, record the case outcome as appropriate. Unlike SARs or FOI requests, you can use the case outcomes 'Action taken', 'Partial action taken', or 'Refusal to take action'.
6. If we agree to take action, you should:
   a. Add a case note to all relevant cases on ICE 360. Explain the restriction, specifying what information is restricted and why. Also send an email to the relevant GMs in PADPCS, FOI Complaints etc, using the template, highlighting the cases where processing has been restricted.
   b. Add a Processing Restriction to the requesters Contact record in ICE 360 following the guidance in the ICE 360 Processing Restrictions Guide.

Other resources: External website - UK GDPR Article 18.

External website - [DPA 2018, Chapter 3, Rights of the data subject](#).

Section updated: 5 June 2023.

Requests for Datasets

Background

We sometimes receive requests for datasets other than those [Complaints and concerns data sets](#) we pro-actively disclose on our website. Datasets should only be disclosed as .csv files as this format does not support hidden data. It is also a machine readable and reusable format.

Task

Responding to requests for datasets that are not pro-actively published.

Steps

1. Where dataset information is requested that is not already proactively disclosed, this will need to be obtained from Operations Service Delivery (OSD) via their request form on Iris.
2. On receipt, check datasets for personal data – this should be done before they are used in a consultation. No personal data should be disclosed as part of a dataset.
3. Case details disclosed online in our existing datasets can usually be disclosed. Other details must not be disclosed without internal and external consultation. See the Requests for data sets - guide for request handlers for disclosable details in ███.
4. Where it would be unreasonably time consuming to consult externally with multiple organisations, you may be able to withhold some details under section 31 FOIA, but this will depend on the exact nature of what is being requested. If unsure, speak with your manager.
5. Information disclosed online as PDF files, such as our income and expenditure, can be converted to .csv files and disclosed in reusable format.
6. All datasets must be converted to .csv files and peer checked prior to disclosure. See the Creating .csv Files section of this manual.

Section updated: 16 May 2023

Operation Cederberg FOI Requests

Background

In May 2017 the Information Commissioner announced an investigation into the use of data analytics for political purposes. The investigation consisted of two main work strands, known internally as Operation Cederberg. The investigation resulted in regulatory action being taken against a number of organisations. At the time, ICO seized information that included personal data. However, once the investigation was closed this information was returned to the relevant organisations, so we no longer hold the personal data seized.

Task

Handling FOI requests about Operation Cederberg, treating them as potentially high profile.

Steps

1. Treat the request as potentially high profile, following the High Profile Request Alert Procedure.
2. Search Cederberg folders for information in scope: Operation Cederberg, and Operation Cederberg 2. Authorisation to access these folders can be provided by Heads of Investigations (see Key contacts below).
3. Do not create copies of in scope information on the request case, but do ensure there is a note on the case specifying where the information is held.
4. Consult Heads of Investigations about the request, and secure their approval of the request response.
5. Once approved, distribute to the high profile alert list.
6. Issue the response to the requester.

Key contacts: Head of Investigations - Andy Curry.

Section updated: 19 February 2024.

Operation Motorman Requests

Background

Operation Motorman was an early 2000s ICO investigation into allegations of DPA 1998 offences committed by (amongst others) public sector staff, journalists and private investigators. Police and other public and private sector employees were found to have been selling personal data from sources such as the Police National Computer, the DVLA and BT to private investigators, who in turn were selling the information to journalists.

The ICO did not bring any prosecutions for the reasons outlined in two reports published in 2006: What Price Privacy? and What Price Privacy Now?, but did provide evidence to the 2011/2012 Leveson Inquiry.

As well as our own investigation files, the ICO is the data controller for the information seized during the investigation. Those concerned that their personal information may have been illegally obtained and shared can make a SAR to the ICO.

We also occasionally receive FOI requests for information held relating to the investigation, requests for assistance from other law enforcement agencies in compiling evidence for their own criminal cases, and enquiries relating to other civil cases.

All information requests and enquiries relating to Operation Motorman should be passed to the designated IA Officers listed under Key contacts below.

Task

To process and respond to Operation Motorman related SAR and FOI requests, and related enquiries.

Operation Motorman inbox

1. The Motorman inbox is a sub-folder of the IA Team inbox, named 'Motorman requests'.
2. IASOs will manually transfer Motorman-related emails and requests to this sub-folder from the IA inbox.

3. Designated IA Officers monitor the sub-folder weekly for new requests and enquiries. IASOs may also alert them to new requests and enquiries, but it is the Motorman IA Officers responsibility to check and administer the inbox.

Subject access requests

1. Due to the confidential nature of the information, all records and correspondence relating to Motorman SARs are held in ███████████████████████████████, and are not processed in ICE 360.
2. The Operation Motorman Subject Access Procedure is held in this restricted area of SharePoint, accessible to all IA Managers and the designated IA Officers.
3. Handle Motorman SARs as a priority. Record the request in the Motorman SARs Log.
4. Searches of the spreadsheets where details of the primary evidence seized are transcribed should be carried out as soon as possible.
5. If these searches establish information in scope is likely to be held, liaise with the Criminal Investigations Team to access the original evidence.
6. Once our final response is sent, all correspondence must be saved to the SharePoint folder and the SARs log updated.

FOI requests

1. FOI requests for Motorman information are not considered confidential, and can be processed as with any other FOI request within ICE 360.
2. However, the designated IA Officers will need to complete the separate Motorman FOI Requests Log in the SharePoint folder.

Enquiries

Enquiries relating to the Motorman investigation are referred to and dealt with by the designated IA Officers or Managers, and if necessary in collaboration with the Criminal Investigations Team.

Other resources: External website - What Price Privacy? and What Price Privacy Now? (National Archives).

External website - Leveson Inquiry - Report into the culture, practices and ethics of the press - GOV.UK.

Key contacts: Antonia Swann; Rob McCarten.

Section updated: 20 June 2023.

Processing TCA Requests

Background

In 2009 the ICO seized personal information from an organisation called The Consulting Association (TCA). The seized information relates to over 3,000 construction industry workers. These workers had their prospects damaged by the unlawful processing of their personal information. As a result regulatory action was taken against TCA.

Task

To process and respond to TCA related SARs and FOI requests.

TCA request allocation

TCA request cases will be created, allocated and progressed in ICE 360. TCA requests form part of our caseload and count towards team performance. As soon as you receive a new request, check if we hold any data on the TCA database. All TCA information should be held in ICE 360, SharePoint, and safe ███. Please note that TCA requests progressed prior to June 2023 are stored in SharePoint only.

The TCA database

1. Open The TCA Database from SharePoint, for the password get in touch with key contacts.
2. Search for the name of the individual using CTRL + F.
3. Check both tabs 'TCA index' and 'Jubilee Line Extension' (JLE) for matches.
4. When a name match is found, this means information is probably held about an individual.
5. The individual then needs to provide supporting information so we can progress an access request and supply any relevant personal information:
   - National Insurance number
   - ID (copy of a passport or driving license)

- Proof of address (recent bill)
- List of previous addresses

6. It may also be necessary to ask for further supporting information, such as an individual's trade, to identify a definite match.
7. If no name match is found, a No information held response should be issued. This can be done either verbally or in writing.

Verbal requests

We log all calls about TCA, whether we hold information about a person or not. Check the TCA database for a name match. Then log the call by completing the TCA call log.

Written requests

When supporting information has been supplied, we log a written TCA request whether we hold information about a person or not. Log the request by completing the TCA requests log.

The TCA database is for searching. The casework management system ICE 360 holds request communications and responses. The TCA requests log is where some key information about requests is recorded. We log requests because it helps us identify duplicate requests and whether a reasonable interval has elapsed between requests.

Other resources: External website - Ian Kerr sentencing (National Archives) and 14 Enforcement Notices Construction Firms (National Archives) (for background).

External website - IRQ0681617 (National Archives) (for FOI request for all information).

Key contacts: Aideen Oakes, Steph MacLeod, Gemma Lowndes

Section updated: 21 June 2023.

Responding to TCA requests

No information held

If no name match is found, a No information held response should be issued. This can be done verbally or in writing.

Information held

1. Log request in the TCA requests log once supporting information has been received.
2. Note the Construction Industry Database (CID) number from the TCA requests log. The CID number should be sequential and a unique reference for each request.
3. Scope the information held by looking at the relevant entry from the TCA database.
4. Check any hard copy TCA record card stored in safe ██. Scans of TCA record cards stored in safe ██ are also available in SharePoint.
    *   Seized Info: Cards A-L - All Documents
    *   Seized Info: Cards L-Z - All Documents
5. Review and prepare record card for disclosure, redact any third party personal data.
6. Certain TCA database entries are colour coded. Maintain the colour of the entry when including in a response because the colours have a meaning.
7. Generate a response letter using the applicable 'information held' TCA template letter, three standard templates are linked below.
    *   Basic information held only
    *   Basic information held, plus JLE
    *   JLE information held only
8. Send responses from ICE 360 and include the CID number as well as the ICE 360 case reference number in the communication. Send postal responses tracked.
9. Log the date the TCA request was completed in TCA requests log.

FOI requests

We may also receive FOI requests from solicitors, trade unions and the media relating to TCA. Some official information about the investigation and subsequent regulatory action has been disclosed. The relevant FOI response IRQ0681617 is linked under other resources.

Other resources: External website - Ian Kerr sentencing (National Archives) and 14 Enforcement Notices Construction Firms (National Archives) (for background).

External website - IRQ0681617 (National Archives) (for FOI request for all information).

Key contacts: Aideen Oakes, Steph MacLeod, Gemma Lowndes

Section updated: 21 June 2023.

Data Sharing Cases

Background

We receive requests from other law enforcement and regulatory bodies conducting their own investigations. Such requests cannot be handled under the FOIA or other access legislation as they may involve personal data of a third party or information not appropriate for wider disclosure. These cases are handled outside ICE 360.

Task

Recognising and handling a data sharing request.

Summary

1. Data sharing cases might involve requests from police forces, regulators, commissions, professional bodies, or government agencies investigating an individual or business (this list is not exhaustive).
2. IASOs will set up data sharing cases in the Information Access Restricted Cases area in SharePoint. A shell case in ICE 360 is not required.
3. If you are allocated a case in ICE 360 that you believe should be a data sharing case but has not been set up as such, inform your manager.
4. Data sharing cases should only be allocated to SIAOs or TMs.
5. Refer to ██████████████████████████████████ IA data sharing cases procedure for full guidance on handling a data sharing case, along with the [Data sharing code of practice](#) on the ICO website.

Section updated: 14 March 2023.

Restricted Cases

Background

ICE 360 is accessible to most colleagues across the ICO, so requests that have a high level of sensitivity or confidentiality should be handled outside ICE 360.

Task

Recognising and handling a restricted case.

Summary

1. Restricted cases might be requests from current or former ICO employees, whistle-blowers, individuals of significant public interest, or requests in relation to gender recognition cases (this list is not exhaustive).
2. IASOs will set up restricted cases in the Information Access Restricted Cases area in SharePoint, with only a shell case being created in ICE 360. A shell case will not contain a copy of the request or any PD.
3. If you are allocated a case in ICE 360 that you believe should be a restricted case but has not been set up as such, inform your manager.
4. Restricted cases should only be allocated to SIAOs or TMs.
5. Refer to ███████████████████████████████ IA restricted cases procedure for full guidance on handling a restricted case.

Section updated: 14 March 2023

Gender Recognition Certificate (GRC) Related SARs

Background

The Gender Recognition Act 2004 allows transgender people to apply to the Gender Recognition Panel to seek full legal recognition of their acquired gender. If successful, they will be issued with a full or interim Gender Recognition Certificate (GRC). The Act also prohibits the disclosure of someone's gender history and the fact that they have applied for a GRC. Disclosure is a criminal offence.

Gender reassignment is a protected characteristic under the Equality Act 2010.

Task

Handling information requests from a person with a GRC.

Steps

1. Only take exceptional steps if a requester has explicitly told us they have obtained or have applied for a GRC, they have provided us with a copy of their GRC, or if in some other way we have been actively informed that we are now holding protected information.
2. Process the request as a restricted case (see Manual section on Restricted Cases). If the request is for personal data, consider that there may be information in scope held in restricted areas of SharePoint.
3. Refer to Annexes J-M of the ICO Trans Policy and Guidance when handling a GRC-related request.

Section updated: 24 January 2024

Requests From Current or Former ICO Staff and Trade Unions

Background

ICE 360 is accessible to most colleagues across the ICO, so requests from current and former employees and Trade Unions that typically attract a higher level of sensitivity are handled outside of ICE 360 and should follow the process below.

Task

Handling requests from current/former ICO employees and the Trade Unions

Steps

1. IASO sets up the request case in accordance with ████████████████████████████ ████████ IA restricted cases procedure.
2. IASO informs the SIAO designated to deal with this type of request (and their manager), then assigns the SharePoint and ICE 360 shell case to them unless advised to do otherwise.
3. IASO saves a copy or summary of the request to the folder in SharePoint and deletes any copy in the IA inbox.
4. IA Officer sends a request acknowledgement to the requester via Outlook, informing them that their request will be handled in accordance with the restricted cases procedure.
5. Consultations about SARs are sent via Outlook using 'Sensitive: Staff SAR' in the title.
6. As with all other FOI requests, consultations should not identify the requester, but they should be sent via Outlook, not ICE 360.
7. IA Officer sends response and disclosure to requester via Outlook. Postal responses will be printed and sent by the designated SIAO where possible and will not be sent to the shared inbox for the wider team to post.

8. IA Officer uploads all relevant information to SharePoint only, then marks as complete on SharePoint and ICE 360.
9. Internal reviews and service complaints for these types of requests should be dealt with by a GM within SharePoint (rather than in ICE 360). Any follow up correspondence should also be saved to SharePoint.

Key contacts: Sarah Coggrave (Designated SIAO), Ian Goddard.

Section updated: 06 April 2023.

Managing PDF Files Using Adobe Acrobat

Introduction

This chapter explains some of the most used Adobe Acrobat functions you are likely to need in the course of your work in IA. Remember, all responses issued electronically should be disclosed as PDF files (except datasets which can be issued as .csv files). This chapter will explain just one method for each task, but there are usually multiple methods you can use. If you prefer a different method to what is written here, please continue to do so.

Deleting Multiple Pages From a PDF File

Task

Deleting more than one page at once from a PDF file using Adobe Acrobat.

Steps

1. Open your PDF file in Adobe Acrobat.
2. Open the 'Organize Pages' function: Tools > Organize Pages, or click the icon in your menu bar.
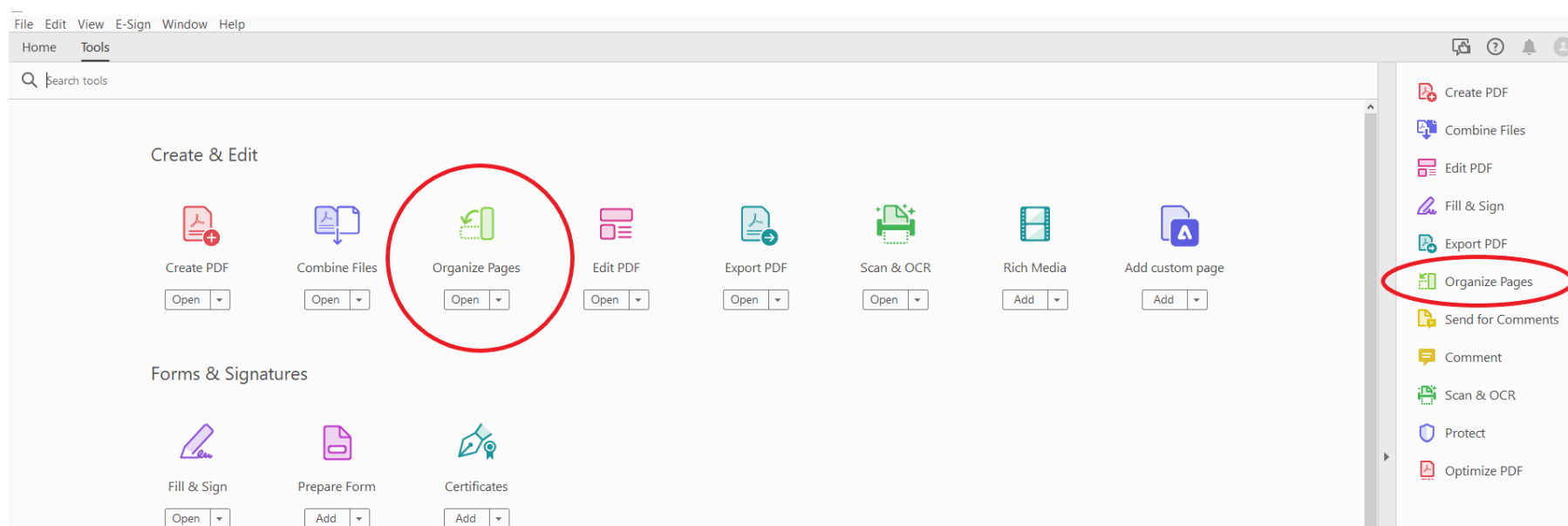
3. When you open the 'Organize Pages' function the view changes to show all pages in the document.
4. There is a zoom function in the bottom right corner; move the blue arrow along the scroll bar to increase or decrease page size.

5. To delete multiple pages, click the 'Enable multiple page selection' checkbox in the bottom left corner.
6. Select all the pages you want to delete by clicking on them. Selected pages will be highlighted.
7. Check the correct pages are selected and click 'Delete' (dustbin icon at the top of the screen).
8. When finished, click 'Close' in the top right corner.

1.
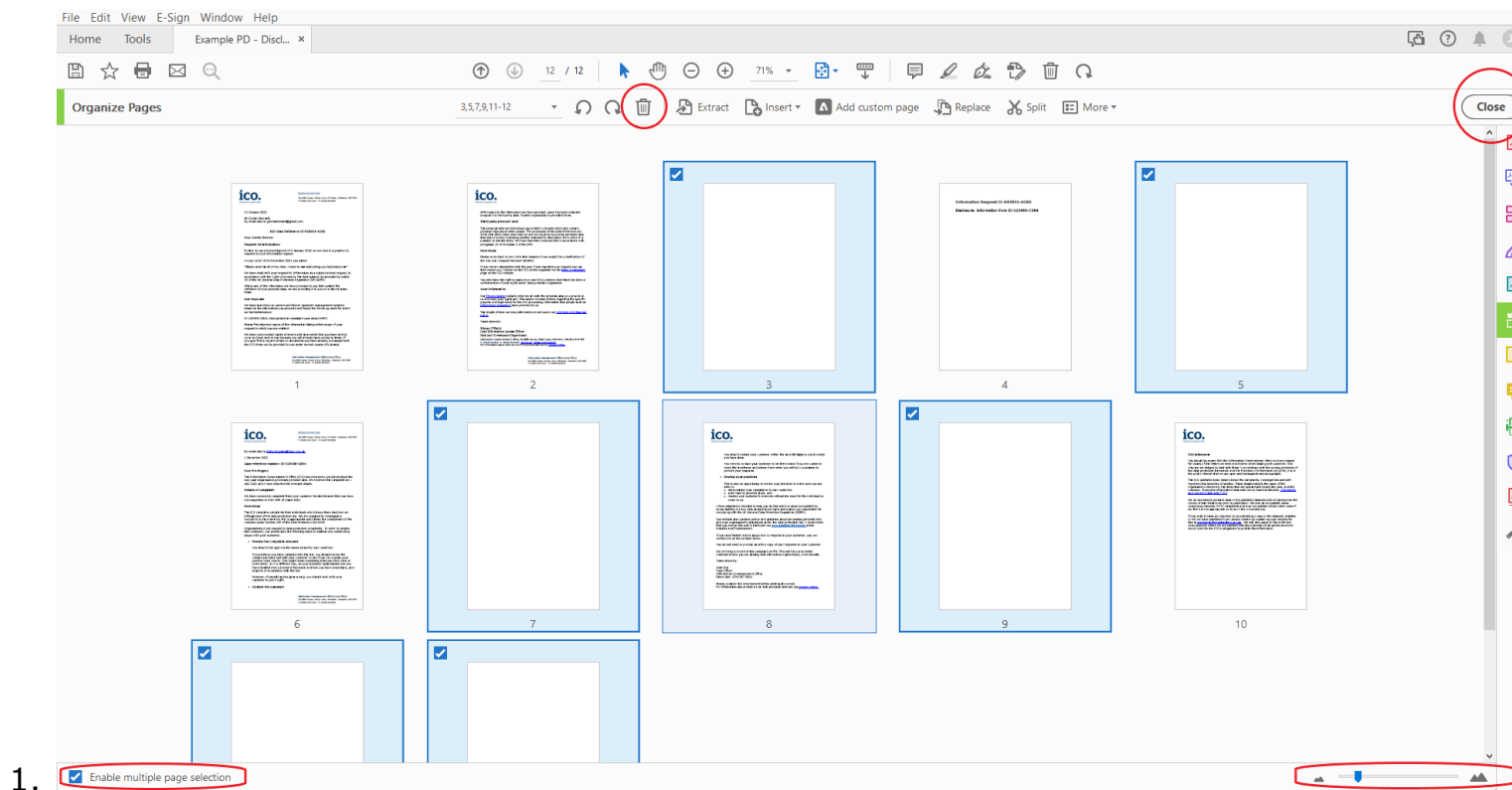
Other resources: External website - Adobe Acrobat User Guide.

Key contacts: IT Help.

Section updated: 11 October 2022.

Inserting Pages in PDF Files

Task

Insert pages into a PDF document; either blank pages, or another PDF file

Steps

1. Open your PDF file in Adobe Acrobat.
2. Open the 'Organize Pages' function: Tools > Organize Pages, or click the icon in your menu bar.
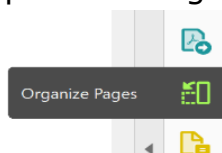
3. Click on the page preceding where you want to add pages.
4. Select 'Insert' at the top of the screen.
5. From the drop-down menu, select 'Blank Page' if you want to add a blank page or 'From File' if you want to add a different document.
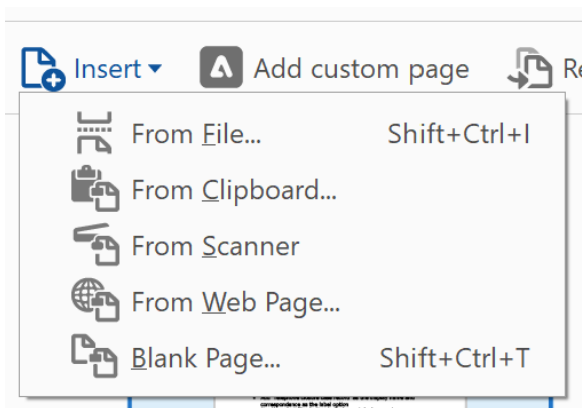
6. In the 'Insert Pages' dialogue box, ensure that 'After' is selected from the drop-down menu next to 'Location.'
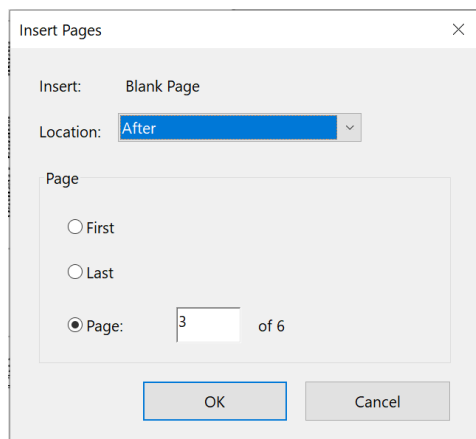
7. Click 'OK'.

Section updated: 19 January 2023.

Combining PDF Files in Adobe

Task

Combine multiple PDF files into a single document in Adobe Acrobat.

Steps

1. Ensure you have no open PDF files. Open Adobe Acrobat.
2. Open the 'Combine Files' function: Tools > Combine Files, or click the icon in your menu bar.
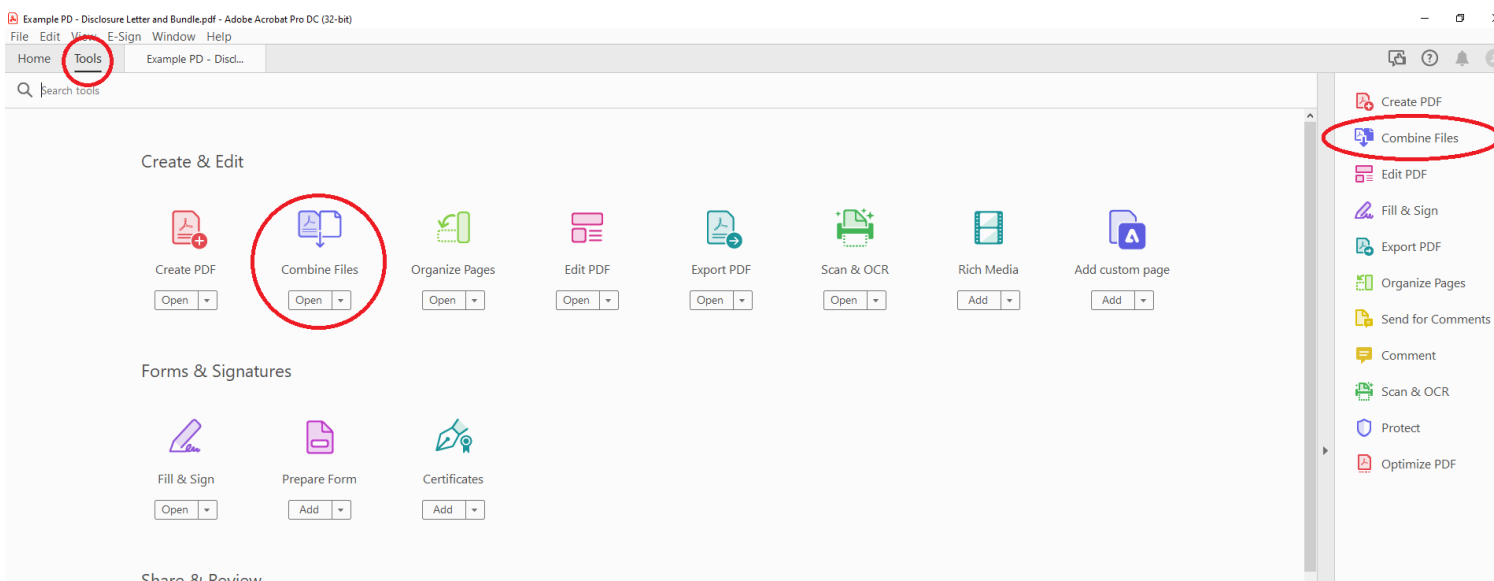
3. Click 'Add Files'.
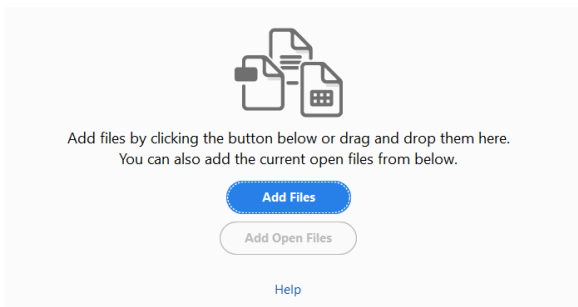
4. This will open a dialogue box. Navigate to and select the files you want to combine. Then click 'Open'.
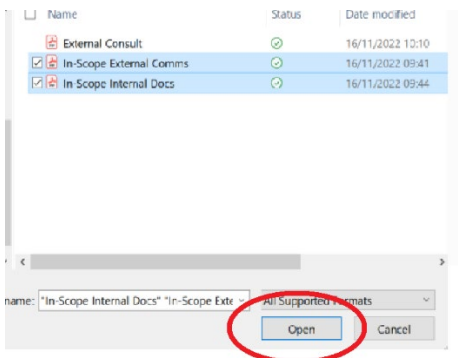
5. If you need to add more documents, select 'Add Files' at the top of the screen, select 'Add Files' from the drop-down menu, and repeat steps 3 and 4.
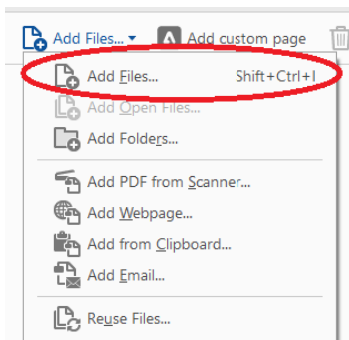
6. The documents selected will show in the order they will appear in the combined document. Click and hold to drag and drop the files to re-order them, if necessary.

7. Click the blue 'Combine Files' button at the top right-hand of the page. This will create a new document titled 'Binder 1'.
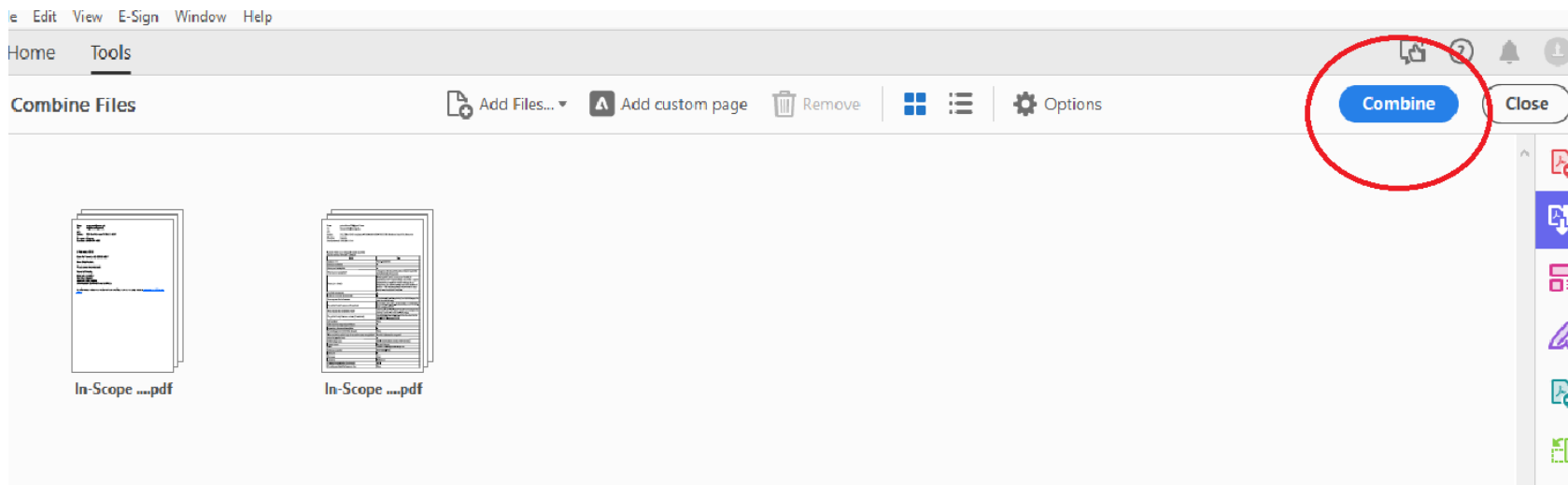
8. Save the document with a new name.

Section updated: 16 November 2022.

Importing Redaction Codes to Adobe

Task

To import redaction codes for UK information legislation to Adobe Acrobat. Once you have done this, it is quick to label the redacted information with the relevant exemption you are applying.

Steps

1. Ensure you have 'Adobe - UK FOIA Redaction Codes.xml' and 'Adobe – UK GDPR-DPA Redaction Codes.xml' saved where you can access them. These can be found in ███████████████████ ████████████████████ .
2. Open any PDF document in Adobe Acrobat, then select the Tools tab > Protect and Standardize > Redact.
3. Select any text to apply redactions (it does not matter what text you select – we just need to do this to access the right click menu on the redaction itself).
4. Right click the redaction and choose Properties.
5. Ensure 'Use Overlay Text' is selected.
6. Ensure the Redaction Code radio button is selected.
7. Click Edit Codes > Import Set.
8. Navigate to where you have saved 'Adobe - UK FOIA Redaction Codes.xml'. Select it and click open. This will import the FOIA exemption set.
9. Navigate to where you have saved 'Adobe – UK GDPR-DPA Redaction Codes.xml'. Select it and then press open. This will import the GDPR/DPA exemption set.

Section updated: 26 April 2023.

Applying Redactions to PDF Files

Task

To permanently redact information from PDFs, and to label the redactions with the reason for withholding.

Steps

1. In Adobe Acrobat, go to Tools > Protect and Standardize > Redact.
2. Select the text for redaction by highlighting with the cursor. A red box will appear around the text.
3. If you make a mistake, right click on the red box, then select Delete to remove.
4. The redacted area fill colour defaults to black. To change this, hover the cursor over a red box > right click > select Properties. Click the 'Redacted Area Fill Colour' box to open the colour menu.
5. Use black redactions for exemptions, white redactions to denote out of scope information.
6. Label each redaction to explain why it has been redacted, unless only one exemption has been applied throughout the disclosed information.
7. To label a redaction with the relevant exemption code, right click it and select the exemption from the pre-populated menu. Or you can right click and select 'Properties' to apply a bespoke label.
8. Once you have selected all text for redaction and added your labels, click the blue 'Apply' button in the top right of the screen.
9. A pop up will appear called 'Apply Redactions'. Approve the option to sanitize and remove hidden information before clicking continue.
10. Save the redacted version of the PDF to an appropriate location, using a new name. The redacted version should look something like the below:

By email only to `Sch 2 Prt 3 Pr 16 - Protection of rights of others`

1 December 2021

Case reference number: IC-123456-C3D4

Dear `Sch 2 Prt 3 Pr 16`

The Information Commissioner's Office (ICO) has received a complaint about the way your organisation processes personal data. We received the complaint on 1 July 2021 and I have attached the relevant details.

This information is out of scope

Details of complaint

11. Keep the earlier version, with the proposed redactions unapplied, as an audit copy.

Section updated: 26 April 2023.

Sending Responses

Introduction

The majority of our information request responses will be sent electronically, with any attachments being PDFs. This chapter covers those situations where a response may need to be sent outside email, such as by post or via social media, where any disclosure needs to be made as a dataset, or where correspondence requires translation to or from Welsh.

Sending a Response by Post

Task

Sending a response to an information request by post when the requester has not provided an email address, has specifically requested a postal response, or when the information can only be provided in hard copy.

Steps

1. Upload your response letter and information disclosure documents to your case in ICE 360.
2. Label these documents clearly, pre-fixing the label with 'PRINT'.
3. Complete ██████████████████████████████ Printing for Information Access email form (full instructions on how to complete it are within the form).
   a. Opening this email form prompts an error message in the browser. Ignore this. Click Keep > Open file, to download the email form.
4. SARs must be sent by recorded delivery – specify this on the email form.
5. FOI responses can be sent standard delivery.
6. The email form when sent will go to a sub-folder of the IA Inbox named 'Post Responses – For Printing'.
7. IA Team members attending the ICO office will check this sub-folder, print, pack, and give the response to Facilities, specifying if Recorded Delivery is required. Facilities will notify you of any tracking reference if applicable.
8. Close your case only when you receive notification (from either facilities or a colleague in IA) that the response has been sent. Send a copy of the notification email to your case in ICE 360.

Key resources: ██████████████████████████████.

Key contacts: IASOs.

Section updated: 11 October 2022.

Welsh Correspondence

Background

The Welsh Language Act 1993 compels organisations in the public sector that provide services to the public in Wales to treat Welsh and English on an equal basis. If someone writes to us in Welsh we must reply in Welsh unless they have indicated otherwise.

Much of the ICO website can be viewed in Welsh at Swyddfa'r Comisiynydd Gwybodaeth (ICO).

Task

Have correspondence translated from English to Welsh or vice versa.

Steps

1. Email the correspondence as a Word document to Wales@ico.org.uk.
2. The Welsh office will arrange for translation and will return it to you once translated.
3. When asking for an information request response to be translated from English to Welsh, you should include both the response letter and covering email for translation.
4. Save both the English and Welsh copies of your response to your case in ICE 360, and send the Welsh versions to the requester.
5. You do not need to translate an information disclosure in to Welsh if the information held is only in English.
6. Ensure to leave ample time for translation before a response is due to prevent a late response.

Section updated: 24 November 2022.

Requests via Social Media

Task

Respond to FOI requests received by the ICO via social media channels.

Steps

1. All ICO social media is handled via a platform called Hootsuite.
2. IASOs triage requests sent to us via social media using Hootsuite, and set up the cases in ICE 360.
3. Once the case has been set up in ICE 360, handle it as normal.
4. Prepare an anonymised response in a PDF file.
5. Follow the procedure for uploading the response to the Disclosure Log, specifying that the response is for Twitter etc.
6. Once the response has been uploaded to the Disclosure Log, the IASOs will arrange for a response to be sent via social media to the requester with a link to the relevant section of the Disclosure Log.
7. Do not respond to SARs submitted by social media. If a SAR is received via social media the IASOs will reply to explain that we do not respond to SARs this way. They will advise the data subject to contact us directly.

Other resources: ██████████████████████████████ Information Access Team Twitter Procedure and Information Access Team Post Instructions (pages 3-5).

Section updated: 21 December 2022.

Sending Prisoner Correspondence

Task

Send correspondence to prisoners using our Confidential Access procedure.

Steps

1. Correspondence can be signed from 'Information Access Team', with your name and direct dial removed.
2. Place the letter and information disclosure to the prisoner in an envelope (envelope A).
3. Label envelope A with the prisoner's name and number. Stamp envelope A with "From the Information Commissioner's Office and subject to the Confidential Access Procedure" (Stamps are available in the office with this wording).
4. Place envelope A in a larger envelope (envelope B) with the appropriate covering letter to the Governor of the prison. Templates are in ███████████████████████████████████. Note that we use a different covering letter to prisons in Scotland compared with the rest of the UK.
5. Address envelope B to the prison's Governor (or equivalent).
6. Post using the IA standard postal procedure: ███████████████████████████████████████.

Other resources: ███████████████████████████████ Prisoner Communications Procedure.

Section updated: 14 November 2022.

Creating .csv Files

Background

We sometimes disclose datasets other than those we pro-actively disclose on our website. Datasets should only be disclosed as .csv files as this format does not support hidden rows and columns, hidden data, pivot tables etc. This reduces the likelihood of mistakenly disclosing sensitive or out of scope data.

Task

Disclosing datasets in a safe, usable format.

Steps

1. If necessary, delete unwanted tabs, columns and rows from the Excel (.xlsx) file. Do not hide or filter information to remove it.
2. Amend data fields, edit column headings, sort data etc to present the data in a logical format that can be easily interpreted by the requester.
3. File > Save As > name and save the file in 'CSV (comma delimited)' format.
4. If the source Excel spreadsheet has multiple tabs you will need to save each one as a .csv file separately. Copy and paste each tab into a separate file and save as a .csv file.
5. Check the file and ask a colleague to check it before disclosing (see the next section).

Other resources: ███████████████████████████████ Guide – creating CSV files.

Section updated: 14 April 2023.

Checking .csv Files

Background

Before disclosing .csv files, each IA Officer should check their own files, and then email the IA Team to request a colleague double check each file too.

Task

How to check datasets to be disclosed for yourself or for a colleague.

Steps

1. Ensure each file name ends with .csv.
2. Open the document > File > Info > Inspect workbook/check for issues > inspect document.
3. Ensure that every box in the pop up is ticked, then click 'Inspect' ('Ink' is usually unticked, so this will need ticking).
4. Flag up any warnings shown here (except the below) to the IA Officer.
5. There will always be the warning re 'Document Properties and Personal Information' that says 'Absolute path to the workbook'. Ignore this.
6. Then do a visual check on the whole dataset itself. Filter the columns if needed to ensure there is no personal data or other data that should not be disclosed. Flag up any problems to the IA Officer.

Other resources: ██████████████████████████████████████ Guide – creating CSV files.

Section updated: 14 April 2023.

After Responding

Introduction

Once your response has been sent and you have closed your case in ICE 360 there may still be further work to do. Appropriate FOI responses should be added to the ICO Disclosure Log, and requesters may reply to our response with queries, a request for review, or a complaint.

This chapter covers our approach to these, but you should also speak to your line manager if you have any concerns regarding a reply from a requester.

Disclosure Log – Adding Request and Review Responses

Task

Prepare and send FOI, EIR and internal review responses to be added to the ICO Disclosure Log (DL).

Steps

1. Check disclosure against ████████████████████████████████████ Disclosure Log Criteria. Most responses should be added to the DL.
2. Check that your response does not include *any* personal data; the requester's, your own, or anyone else's.
3. Save the anonymous response on the case in ICE 360.
4. Send the response to the requester as normal, including your signature block on the covering email.
5. Ensure you select 'yes' for the 'Proactive disclosure' option when closing the case in ICE 360. (If you are *not* adding the FOI response to the DL, ensure you add a case note to the case to explain why.)
6. Fill out the relevant Outlook Disclosure Log Submission Form, either for a request response or an internal review response. Attach a copy of the response as well as any disclosure documents.
7. An IASO will send this to Website Updates to be added to the Disclosure Log and will update the tracker spreadsheet on SharePoint to show that this has been done.

Other resources: ████████████████████████████████████.

            ICO website - Disclosure Log.

Section updated: 30 January 2024.

Service Complaints

Task

Handling a service complaint in ICE 360.

Steps

1. Alert all IA Managers (█████████████████) that a service complaint has been received.
2. Identify which IA Manager will consider the service complaint.
3. In ICE 360 go to the grey ribbon on the request case, select New > Review > Service Review.
4. Record the details for the service complaint in the activity screen (date complaint received, reviewing officer, case officer, primary and secondary reason for complaint) and save them. A service review activity will be created on the case. The case will remain in your work queue if it is still open.
5. Acknowledge the requester's service complaint as soon as possible, and within 14 days of receipt as per the ICO Service Complaints Policy.
6. Advise the complainant of the service standard for a response (within 30 calendar days).
7. Email the designated service complaint handler with the case reference and service complaint response due by date.
8. The service complaint handler must complete the service review activity on the request case once they have issued a response.
9. The service complaint handler should notify the original IA Officer of the service complaint outcome.

Other resources: ████████████████████████████████ IA ICE 360 case handling procedure.
ICO website - Service complaint policy.

Section updated: 11 January 2023.

Internal Reviews of FOI Requests

Task

Handling FOI and EIR internal review requests in ICE 360.

Steps

1. If a requester makes contact to express dissatisfaction with a response an internal review will usually be required. Please note requesters do not necessarily have to ask for an internal review – an expression of dissatisfaction with the response is enough for this process to be triggered.
2. Alert IA Managers that a request for internal review has been received.
3. Identify with IA Managers who will conduct the internal review.
4. Acknowledge the internal review request using the email template in ICE 360 named 'Ack-internal review req'.
5. Set-up an internal review activity on the completed request case.
6. To do this, go to the grey ribbon, select new, then internal review.
7. Assign the review activity to the reviewer. An internal review activity will be created, and the case should appear in the reviewer's work queue.
8. Go to the Case: Activities tab and select reviews, select the review link, complete the information for the internal review.
9. Go to the Case: Information screen and amend the case summary to show the internal review due date.

The FOIA or EIR element of a hybrid response can be considered as part of an internal review.

Other resources: SharePoint - ICE 360 request handling procedure, Procedure – receiving review request.

Section updated: 19 January 2023.

Preserving a Case in ICE 360

Background

We may need to mark a case for preservation so that it is not deleted in line with our usual retention period because, for example, it relates to an open public inquiry, ongoing legal action, or current information request.

Task

Preserve a case in ICE 360.

Steps

1. If you know the case needs to be preserved when you close the case, click 'Yes' for 'Preserved' in the Complete Case box that appears during the case closure process.
2. If you need to preserve a case that has already been closed, locate and open the relevant case in ICE 360.
3. Go to the 'Case: Information' tab using the drop down above the case reference in the top-left corner.
4. In the 'Summary' section, there are three boxes. In the right-hand box is a field titled 'Preserved'.
   a. If the field is set to 'No', click it once to change it to 'Yes'.
5. A new field will appear titled 'Preservation reason'. Select the relevant reason from the drop down menu.
6. Once you have selected a reason, click 'Save'. The case is now preserved.
7. Send a case note to the case with brief details about why the case has been preserved.

Key contacts: LIMO - Antonia Swann.

Section updated: 2 January 2024.

Requesters

Introduction

We have policies and procedures in place to assist us in ensuring that interactions with requesters are positive and productive. We must always be mindful of the welfare and individual needs of requesters when responding to information requests. We must also be mindful of ICO staff welfare and the need for communications to be handled by the appropriate contact to ensure they are progressed appropriately.

This part of the manual covers our approach to interacting with requesters, but you should also speak to your line manager if you have any concerns or queries regarding the welfare of a requester, your own welfare, or our responsibilities in making information accessible.

Addressing Requesters

1. When addressing the requester directly, you should either use their full name or their first initial and last name eg 'John Smith' or 'J Smith'.
2. Avoid using gendered titles such as Mr and Ms when referring to individuals, unless it has been made clear that the requester uses those titles. Similarly, when referring to a requester in the third person, use gender neutral language such as 'they' unless it has been made clear that the requester uses other specific pronouns.
3. Professional titles such as Dr should be used where it has been made clear that the requester uses that title. The same is true for suffixes such as MSc or OBE.

Section updated: 8 March 2023.

Making Documents Accessible

Task

Make all documents accessible and easy to read.

Steps

1. Any document you create, including correspondence with requesters and data controllers, should follow the corporate style and be written clearly and concisely.
2. The corporate font is Verdana 12pt. Georgia 14pt should be used for headings, and Verdana 12pt bold can be used for subheadings.
3. You should ensure that you review the ICO Style Guide, which outlines the corporate style in detail.
4. Care should be taken with the needs of some requesters who may have reasonable adjustments. Documents can be provided in larger font sizes, a different font, or on coloured paper if necessary.

Section updated: 16 May 2023.

Reasonable Adjustments

Background

Under the Equality Act 2010, public authorities must make reasonable adjustments in their approach or provision to ensure that their services are accessible to all people; for example, sending correspondence in a larger font or on coloured paper.

Task

Handling a request for a reasonable adjustment from a customer.

Steps

1. When a customer requests a reasonable adjustment, establish their requirements and agree what is the best reasonable adjustment to make.
2. Record the reasonable adjustment using the service adjustment request form available at Service Adjustments.
3. When the form has been completed email it to PADPCS (see email address and full instructions at Service Adjustments. The authorising manager will add it to the list of reasonable adjustments once approved.
4. Check the Reasonable Adjustments list routinely to ensure that reasonable adjustments are followed when issuing request responses.

Other resources: ICO website - ICO reasonable adjustment policy.

Section updated: 8 February 2023.

Requester Welfare

Task

Handling a customer who threatens suicide, self-harm or is otherwise at risk of physical harm.

Steps

1. Threats of harm, either to themselves or others, could be made by someone verbally or in writing.
2. If a customer makes a verbal threat during a phone call, advise the customer that you are not qualified to help and they should seek assistance from emergency services, then end the call.
3. Immediately escalate to your line manager or other senior member of staff, such as another TM or GM, who will make a decision about contacting other authorities, such as the police.
4. Record a detailed case note – any notes of this kind will be considered for disclosure in the event of the customer making a SAR.
5. If a customer makes a written threat, immediately inform your line manager or other senior member of staff, such as another TM or GM, who will again make a decision about next steps.

Other resources: SharePoint - Managing Customer Contacts.

Section updated: 16 February 2023.

Handling Persistent Requesters

Task

Handling a requester who, because of the frequency of their contact, places a strain on time and resources - particularly when there is nothing further that can be done to provide assistance, clarification or resolution.

Steps

1. Check that the internal review and service complaint process has been exhausted.
2. Refer to the ICO [Unreasonably persistent and unacceptable behaviour policy](#) and identify how to proceed with the support of IA Managers.
3. Issue a communication addressing the requester's behaviour. The communication should explain why their behaviour is unreasonably persistent and ask them to refrain from this behaviour in future.
4. Manage their expectations by including: *"We have considered your latest communication and have nothing to add to our previous responses. We now consider the matter closed. As this case is now closed any further correspondence sent to it may not receive a response."*
5. If the requester is persistent in relation to a service complaint, ensure that they have been provided with the next steps available to them i.e. contacting the PHSO.
6. Where unreasonably persistent behaviour continues, an IA Manager will advise the requester that their behaviour could result in access to services being restricted. The restriction of access to our services by creating a restricted contact record is covered at section 10 of the ICO [Managing customer contacts](#) procedure.

Section updated: 7 March 2023

Mail Management Inbox

Background

Sometimes we experience significant difficulties with a requester's email correspondence. For example, this might be an unacceptable volume of emails, or abusive language may be used. In these circumstances we can consider creating a Mail Management (MM) inbox folder for that requester which will divert their emails to a specific Outlook folder regardless of which ICO email address the customer used. Other casework departments also use this process, so not all folders in the MM inbox will have been set up by IA.

As the MM inbox is restricted to those who require access only, it can also be used to divert messages from Protected Persons, or others who require additional privacy or confidentiality.

Task

To create a Mail Management inbox folder.

Steps

1. Obtain the approval of IA GMs to add someone to the Mail Management system.
2. Once approval is obtained, compile the necessary information for IT:
    a. Customer's full name.
    b. Name of inbox folder to be created (usually customer first name & surname).
    c. If customer's name should not be in the folder name, say why.
    d. Email address(es) the customer uses to contact us.
    e. Reason for request.
    f. Name(s) of ICO colleagues to be given access to the folder.
    g. Line manager (also to be given access).
    h. Authorising manager (if different to above).

3. An IASO will send this information to IT Help to ask for the folder to be created, copying in the IA Officer who has requested it, the GM who approved it, and a SPoC if relevant.
4. An IASO will add the details to a tracker held by PADPCS.
5. IASOs will monitor the relevant MM folders, forwarding emails to ICE 360 or notify IA Officers of relevant emails as appropriate.
6. If you have access to the MM inbox it will show in the list of inboxes in your Outlook email. If you do not have access but need it, contact IT Help.

Other resources:	██████████████████████████████████
	Mail management inbox process.
Key contacts:	IT Help.
Section updated:	9 June 2023.

Protected Persons

Background

We occasionally receive requests for information from members of the public classed as a 'protected person'. Whilst our approach to dealing with these requests remains consistent with any other, it is important to consider the additional risks that may be attributable to a protected person.

Serious Organised Crime and Police Act 2005: Section 88 of this Act imposes a criminal liability when disclosing information that relates to a protected person. This is not dissimilar to the criminal liability attached to section 132 of the DPA. Staff dealing with these requests should therefore take the same approach they would for any other, ensuring we only disclose information when appropriate and lawful to do so.

What is a protected person?

Section 94(3) states that: *A person is a protected person if—*

(a) arrangements have been made for his protection under subsection (1) of section 82, and
(b) the arrangements have not been cancelled under subsection (2) of that section.

Section 82(1) refers to people who are considered at risk. When dealing with information requests this is likely to be people with an assumed identity or in witness protection.

The legislation provides further information to help explain the term 'assumed identity'.

(5) A person assumes a new identity if either or both of the following apply—
(a) he becomes known by a different name;
(b) he makes representations about his personal history or circumstances which are false or misleading.

Risk attached to protected persons

There will always be an element of risk attached to any disclosure made by the IA Team. When progressing a request submitted by a protected person that risk is higher. We should make every effort to reduce risk to an acceptable level. Where we know or suspect, that an individual is a protected person we must be particularly mindful not to disclose any information that indicates an individual has, or might have, assumed a new identity.

Task

Processing an information request from or involving a protected person.

Steps

1. The request should be progressed as a restricted case. This ensures access to the case is restricted to those who have a business requirement to do so.
2. Consider creating a restricted mail managed inbox for the requester. This will allow controlled access and avoid the need to have sensitive information exchanged via the IA inbox. You will need to ensure that any mail management inbox has appropriate access controls in place and that it is monitored regularly so correspondence from that individual is not overlooked.
3. Avoid using the name of a protected person within internal emails and consultations where possible. You should mark any correspondence as 'OFFICIAL SENSITIVE'.
4. When progressing a potentially high profile (HP) information request it is not likely to be appropriate or necessary to share the name of the requester as part of the request alert procedure. In the first instance, simply showing "Protected Person" under the name entry is likely to be sufficient.
5. Care and attention should be given to email addresses used by a protected person. If a requester changes their email address, it may be necessary to complete a security check. This could be difficult if both a birth name and assumed name are being used by a requester. We must not ask for any information that would indicate that they have assumed, or might have assumed, a new identity.
6. If in doubt seek advice from an IA Manager, this will allow decisions to be made on a case-by-case basis.

Section updated: 1 December 2022

Information Access Team Administration

Introduction

The ICO Information Access Team has processes in place to support the core functions of the team. These relate to fair allocation of request cases, covering staff absence, and managing caseloads. Some key aspects of this are covered in the following chapter, and you should use it to understand what your responsibilities are outside of casework.

IA Team Communication Channels

Task

To understand and join the different Outlook mailing lists and inboxes, and Teams groups and channels for IA.

Email mailing lists

1. Sending an email to a mailing list means each member of that lists receives an individual email to their personal inbox.
2. The IA Team has the following Outlook email mailing lists, named in the address book as follows:
   a. Informationaccessteam = The whole IA Team.
   b. IA Managers = Group Managers and Team Managers.
   c. IA Seniors = SIAOs.
   d. IA Leads = LIAOs.
   e. TNA Transfer Team = IAOs who work on The National Archives (TNA) project.
3. All members of the IA Team should appear on the Informationaccessteam list, and other lists as appropriate to their job role and involvement in special projects.
4. Contact IT help if you do not appear on a relevant email list, or if you appear on a list incorrectly.

Email inboxes

1. Sending an email to an inbox means one message is sent to that inbox, but multiple people can access it if they have relevant permissions.
2. The IA Team has access to the following Outlook email inboxes, named in the address book as follows:
   a. AccessICOinformation = The IA Team inbox.
   b. IA Datasets = Inbox for pro-active disclosure of datasets project.
   c. Mail Management = Emails from certain complainants/requesters to any ICO email address will be re-directed here. For example, this may apply to unreasonable persistent or abusive requesters.

3. All members of IA should have access to the IA Team inbox, and other inboxes as appropriate to their role and involvement in special projects.
4. Contact IT help if you do not appear on a relevant email list.

Microsoft Teams

1. The IA Team has the following Microsoft Teams groups:
    a. TGrp_Info-Access_Corporate Affairs and Governance, including:
        i. General channel.
        ii. Team Casework Queries channel.
    b. TGrp_Lead Information Access Officers (for LIAOs only).
    c. TGrp_Proactive Disclosures_Corporate Affairs and Governance (for those who work on the pro-active disclosure of datasets project).
2. All members of the IA Team should have access to TGrp_Info-Access_Corporate Affairs and Governance, and other groups as appropriate to their role and involvement in special projects.
3. Contact a group owner if you are not a member of a relevant Team. (Ask an IA colleague to check who the group owner is).

Key contacts: IT Help for Outlook queries.

Section updated: 20 March 2023.

IA Rotas and Regular Responsibilities

Task

The IA Team operates several rotas. All IA Team members must be aware of their turn on each relevant rota, and arrange cover if they are unavailable.

Rotas

There are a few rotas; not all will be relevant to you:

Leading Request Queries sessions   SIAOs and TMs
Allocation   TMs
Post support for IASOs   LIAOs and SIAOs

Steps

1. Check the All IA Rotas document on a weekly basis – ███████████████████████████ ████████████████ All IA Rotas [Year].
2. Check weekly as the rotas may change according to staff availability.
3. If you are unavailable for a session you have been assigned, contact the IA Team to request cover or speak to your line manager.
4. All team members should appear at least once every three months, usually more frequently. If you do not appear, please speak to your line manager.

Section updated: 8 December 2022.

Post Support

Task

To provide cover and support for the IASO managing incoming post and emails. Each IAO takes a turn on the rota for one working week of support at a time.

Steps

1. Check your turn on the All IA Rota document in ███████████████████████████████ ███████████ All IA Rotas [Year]. Arrange cover if you are unavailable that week.
2. IASOs are responsible for all incoming post and emails, but will contact the designated post support if there are queries. For example, to check if a request is valid, or should be directed elsewhere.
3. Emails in the IA Outlook inbox will have a red flag if the IASO is unsure.
4. You may also need to manage the IA Outlook inbox and IR 'Items available to work on' queue in ICE 360 yourself if an IASO is unavailable for a day or more. Consult with your manager if you have not done this before, and consult ██ IASO Manual.
5. Use ███ IA Post Instructions V2 for guidance on how to manage incoming post and emails.

Section updated: 24 January 2024.

Records Management Monthly Checklist

Task

To manage IA records; minimising risk, protecting personal data, and ensuring compliance with our [Retention and Disposal Policy](#). See below for the monthly checklist for action.

Checklist

At least once each month you should do the following:

1. Preserve significant cases and records. These will include:
    a. Any case in ICE 360 in scope of an information request which is about to be deleted.
    b. Request cases in ICE 360 and associated records subject to an appeal or legal action involving the ICO (eg First-tier Tribunal, Upper Tribunal, Judicial Review).
    c. Request cases and associated records relating to an open public inquiry (eg the Covid-19 Inquiry).
    d. Very rarely a request case or associated record that relates specifically to significant actions or decisions within IA will need to be preserved eg a request response that attracts significant media attention, or a case that led to a change in the interpretation of the law.
    e. Teams – Significant posts or conversations within a Teams chat or channel needed beyond the autodelete period.
    f. Outlook – Significant emails needed beyond the 12 month autodelete period.

Refer to the full guidance in SharePoint on When and how to retain IA cases and records.

2. Delete 'Redundant, Obsolete, Trivial' records (ROT). These will include:
    a. Request case related documents. Ensure all relevant documents are saved to ICE 360 and clearly labelled, and delete any draft or working copies still held on your device when no longer needed.
    b. Project documents. Ensure all final versions are saved to the relevant SharePoint folder. Delete any draft, working or final copies from your device once the project is complete.

c. Teams chats and documents. Review and delete as necessary any files, notes, projects etc. you may have shared to a Teams Channel.
d. Snipping Tool screenshots. These are automatically saved in the Pictures > Screenshots folder on your device (unless this option is switched off). Delete all images from this folder.
e. Downloads folder in File Explorer. Delete all documents from this folder.
f. Recycle Bin on your Desktop. Delete all documents from this folder.

Other resources: ██ Guidance.

██████████████ - Managing Information in Microsoft Teams Guidance, Storage Policy, What Digital Information to Save and Where Guidance.

Key contacts: IA LIMO – Antonia Swann.

Section updated: 1 February 2024.

Reporting an IA Data Breach

Task

What to do in the unlikely event of a data breach by IA.

Steps

1. If you discover a breach or potential breach, immediately notify your line manager or other IA manager.
2. After speaking to a manager, contact Cyber Security to outline the nature of the potential breach. If the advice from Cyber Security is to submit a breach report, do this as soon as possible, and in any case within 24 hours, using the Security Incident report form.
3. Follow all advice given by Cyber Security to mitigate any risk. For example:
   a. If the breach has taken place via email, contact IT Help urgently to check if the email can be recalled.
   b. If the breach is contained in a postal response, contact Facilities (█████████████████) to see if the correspondence can be retrieved.
4. If the data breach is contained within an FOI response and has been sent to our Website Updates team to be published on the disclosure log, contact the team (█████████████████████) and ask them not to publish the response; or if it has been published already, ask for it to be removed immediately.

Other resources: Iris - Security Incident Reporting Guidance, Security Incident Management Policy, Information Security Policy.

Key contacts: Cyber Security Services.

Section updated: 1 February 2024.

Buddy System

Task

Monitoring the request cases for your IA 'buddy' if they are absent from work; acknowledge important case correspondence, and apply any case changes.

Steps

1. Notify your buddy in advance when you are going to be absent (if 3 days or more).
2. When your buddy is absent, check their cases for new correspondence daily.
    a. Go to ICE 360 > Queues > All Open Items, Queue: IR.
    b. Check the 'Worked By' column for your buddy's name to see any new emails sent to their cases.
3. You can also view your buddy's ongoing or closed cases:
    a. Go to ICE 360 > Cases > Current Cases > Filter the Function column by Information Rights Cases.
    b. Order or filter the 'Worked By' column by your buddy's name.
4. You can also view your buddy's recently closed cases:
    a. Go to ICE 360 > Cases > Completed Cases > Filter the Function column by Information Rights Cases.
    b. Order or filter the 'Last Handled By' column by your buddy's name.
5. Acknowledge any new correspondence if necessary and advise of any case changes, e.g. acknowledge if clarification has been provided, and provide the new response due date.
6. Update the metadata if there are any case changes e.g. new due date when clarification is received.
7. Refer any new information requests or internal review requests that are received.

Other resources: SharePoint - Information Access buddy system.

Section updated: 31 October 2022.

Out of Office for Email and Voicemail

Task

Setting 'out of office' (OoO) messages on Outlook email and direct line voicemail in Teams.

Email

1. In Outlook, go to File > Automatic Replies > select 'Send automatic replies'.
2. Input the time that you want OoO replies switched on, and the message to be sent.
3. OoO replies to people outside the organisation should specify that information requests should be forwarded to accessicoinformation@ico.org.uk.
4. You cannot set an OoO message for email sent to your cases in ICE 360. Remember to let your buddy know when you are going to be away so they can monitor correspondence sent to your cases.

Voicemail

1. Click the ellipses (…) next to your profile picture/initials in any Teams window, then click Settings.
2. Click Calls > Configure Voicemail.
3. Set the call answer rules, and greeting language.
4. Set the OoO text-to-speech greeting (limit of 200 characters), or click the 'Record a greeting' button if you wish to record your own message.
5. Set when the OoO message should play. You can switch voicemail on manually, or whenever your OoO message is active in Outlook.

Other resources: ███████████████████ - Microsoft 365 Help.

Section updated: 20 March 2023.

# Recording Planned Absences - IA Calendar in Outlook

Task

Adding your planned absences to the IA calendar in Outlook

Steps

1. You must add any planned absences to the IA calendar in Outlook so your absences can be considered when allocating requests, assigning places on the IA rotas etc.
2. Open Outlook and click the calendar icon in the bottom left corner.
3. Select the 'Calendar – Information Access Inbox' checkbox in the left hand window, and leave the others unchecked.
4. Ensuring you are in the 'Home' tab, click New Appointment in the top left. A new window will open.
5. Complete the details of your absence including your name and Annual Leave or Flexi Leave etc as appropriate for the appointment title, and the relevant dates.
6. Click Categorize in the ribbon, and select 'Annual leave'.
7. Select the check box for 'all day' if you will be absent for the whole day.
8. Do not add location.
9. Once all details are completed, click 'Save and Close.'

Section updated: 13 December 2022
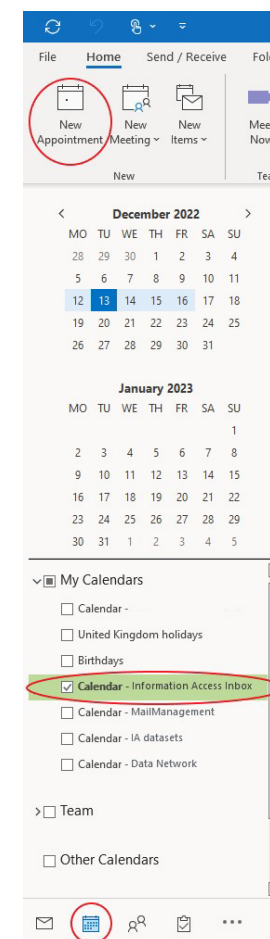
SharePoint Overview

SharePoint is the ICO Electronic Document and Records Management system (EDRM). It is integrated with the intranet (Iris) and casework management system (ICE 360) so documents you see in Iris and ICE 360 are actually held in SharePoint.

Functions

1. The Information Access area of SharePoint is named Access to ICO Information, AI for short.
2. All areas of the ICO use SharePoint to store and share corporate documents, so you may need to search and access SharePoint when scoping requests.
3. Your access to areas of SharePoint is set by IT. You may not have permissions to access some areas.
4. Your ability to upload, add or amend different folders, documents etc will also depend on your permissions. Speak to your line manager if you do not have the required permissions.
5. Only Site Owners or IT can add new sections and sub-sections.
6. Each area of SharePoint has a search bar in the top right corner.
7. Or you can use the 'Enterprise Search' function in the horizontal menu bar at the top of each screen. The Enterprise Search area also provides access to the Advanced Search Tool, and Quick Tips for searching.
8. The search functions search file names, titles (metadata) and content of documents.
9. Although documents attached to cases in ICE 360 are housed in SharePoint, they are not searchable in SharePoint.

Other resources: Search Workday for more in-depth training on using SharePoint.

Key contacts: Ian Goddard, Aideen Oakes, Eluned Cook - Current Site Owners for IA on SharePoint.

Section updated: 21 February 2023.

Request Case Tiers

Task

Assign request cases a tier or rating based on likely level of complexity and/or how time consuming it will be. The tier is assigned when the request case is created (usually by an IASO), but can be amended if required.

Steps

1. Each request case summary in ICE 360 should begin with the case tier; either T1, T2 or T3.
   a. Tier 1 (T1), Potentially quick to resolve eg:
      i. Obviously misdirected requests.
      ii. Requests for a single email on a complaint case.
      iii. Requests for information which we know is already available on the website.
      iv. Requests for information which we know we can disclose immediately.
   b. Tier 2 (T2), 'Normal' requests eg:
      i. SARs for a complaint case file, or an FOI request requiring an internal consult.
      ii. Some internal or external consultation required.
      iii. Will likely require the application of at least one exemption.
      iv. Requests for erasure or rectification (Art 16 or 17 of GDPR).
      v. Request for complaint case files across numerous case reference numbers.
   c. Tier 3 (T3), Complex or high-risk requests eg:
      i. Requests which are likely to be extremely voluminous.
      ii. Requests about big, multi-department ICO projects.
      iii. Require in-depth scoping and lengthy, detailed consultation with other bodies.
      iv. High profile or sensitive cases.

Section updated: 3 November 2022.

IA Pages On Iris

Iris is the name for the ICO Intranet. IA has its own section in the Governance and Planning Hub (███████ ███████████████████████ Information Access – Learn More) that includes useful resources for both the IA Team and the wider ICO. These include:

1. A form to Submit a request referral to Information Access.
2. Information Access guides that provide help on recognising an information request, how to refer a request to IA, and responding to information request consultations from IA and external organisations.
3. A Should I refer to Information Access? tool to help ICO staff decide if something should be referred to IA, if it is actually an enquiry, or if it is a request that can be handled as normal course of business.
4. Find contacts in IA for specialist requests and IA projects.

Key contacts: IA Iris Rep, William Griffiths.

Section updated: 24 January 2024.

The National Archives

Background

[The National Archives](#) (TNA) is a non-ministerial department and official archive and publisher for the UK Government. The ICO website is archived at [UK Government Web Archive](#). This is publicly available and is a useful resource for information requests relating to previous ICO web pages and documents, generally published more than two years ago.

As a public authority subject to the [Public Records Act 1958](#) (PRA) and the [Code of Practice issued under section 46 of the Freedom of Information Act 2000](#) the ICO is required to transfer to TNA archive paper and digital records which are considered to be of significant and enduring public interest.

The IA Team is responsible for selecting, reviewing and transferring ICO archive records to TNA 20 years after closure on a rolling annual basis, where they meet TNA criteria. There is a dedicated SIAO who runs the TNA project and other IA staff can volunteer to assist.

Task

To transfer to TNA suitably prepared and redacted paper and digital archive records which meet the selection criteria, on an annual basis.

TNA process

In line with TNA guidance on [Selecting and transferring paper records](#), and the ICO Transferring Records to the National Archives Procedure, along with other public authorities subject to the PRA, the ICO is required to follow six key steps:

1. Appraisal

This is the review and decision making process around which ICO records should be kept and/or marked for preservation beyond their usual retention and disposal criteria (for example, two years for casework and six

years for legal files), on the basis the record is significant and may be subject to TNA transfer criteria 20 years after completion. Further details are given in ICO Appraisal and Selection Policy.

2. Selection

All records still held by the ICO which reach 20 years of age from 'creation' (ie completion) are reviewed on either a micro (individual) or macro (collection) basis to see if they meet TNA's criteria for transfer. For each record selected for transfer a note is made of the relevant TNA criteria and JX series (ie a set of related records, specific to the ICO). All records not selected for transfer are likely to be securely destroyed.

3. Sensitivity Review

Similar to disclosure under the FOIA 2000, each record selected for transfer is reviewed for any information which should not be made publicly available. Typically, the ICO has only withheld or redacted personal data from transferred records under the s40(2) FOI exemption, but other FOI exemptions may need to be considered. Once we have received approval from the Lord Chancellor's Advisory Council for any proposed exemptions, the exempted information or file is transferred to TNA as a 'closed' record, and is only made publicly available several decades later. Open records with no redactions or some pages redacted are publicly available immediately after transfer to TNA.

4. Cataloguing

All records selected for transfer need to be 'catalogued', where they are listed, referenced and described to the standard required by TNA for inclusion on the online catalogue Discovery. Each record, whether transferred open or closed, is given a unique reference number and, if necessary, also given a new and meaningful file title so that the public can easily understand what type of information is held.

5. File Preparation

All paper records need to be prepared in line with specific archival requirements prior to transfer, to ensure they meet the required physical standard for permanent preservation. For example, bearing in mind the transferred records will be held by TNA for hundreds of years we need to review or remove any parts which will deteriorate

or adversely affect the quality of the physical material held over time. The records also need to be sturdy and secure enough to withstand access by the public when requested.

6. Uplift

Once all the stages described above are complete, the records are then transferred or 'uplifted' securely to TNA. Paper records are boxed up and labelled according to TNA requirements, and the uplift takes place on a specific date agreed with TNA, usually by courier. Digital records need to be transferred electronically using the TNA's current DROID system.

Accession – TNA only

This is the final stage of the process, actioned by TNA once the records have been transferred. TNA take responsibility for the 'accession' of transferred records, ensuring open records are accessible to the general public where appropriate, and closed records are held securely until they too are ready to be made accessible to the public.

Key contacts: Antonia Swann.

Section updated: 23 June 2023.

Feedback on this Document

If you have any feedback on this document, please contact Information Access.

Version History

Version	Changes made	Date	Made by
1.0	Published	30 June 2023	Eluned Cook
1.1	Some sections revised; new sections added	1 March 2024	Eluned Cook