Staff Privacy Notice

Version number: 3.42

Status: Published.

Department/Team: Data and Information Management.

Relevant policies: N/A.

Distribution: Internal.

Author/Owner: Steven Johnston, Team Manager, Data and Information Management.

Consultees: N/A.

Approved by: Helen Ward, Head of Knowledge Services and Internal Communications.

Application date: 31/04/2019.

Review date: 31/01/2027.

Security classification: Official.

Key messages

The main objective of this policy is to provide:

- All ICO employees, ex-employees, agency staff, contractors, secondees and non-executive directors with information about what they can expect when the ICO processes their personal information.

Does this policy relate to me?

The privacy notice applies to all staff.

Table of Contents

1. Introduction

As an employer the Information Commissioners Office (ICO) must meet its contractual, statutory and administrative obligations. We are committed to ensuring that the personal data of our employees is handled in accordance with the principles set out in the Commissioner's Guide to Data Protection.

This privacy notice tells you what to expect when the ICO collects personal information about you. It applies to all employees, ex-employees, agency staff, contractors, secondees and non-executive directors. However, the information we will process about you will vary depending on your specific role and personal circumstances.

The ICO is the controller for this information unless this notice specifically states otherwise. Our Data Protection Officer is Louise Byers, Director of Risk and Governance. If you wish to contact her you can do so using this form or via our postal address.

This notice should be read in conjunction with our global privacy notice and our other corporate policies and procedures. When appropriate we will provide a 'just in time' notice to cover any additional processing activities not mentioned in this document.

Back to the top

2. How do we get your personal data

We get information about you from the following sources:

- Directly from you.
- From an employment agency.
- From your employer if you are a secondee.
- From referees, either external or internal.
- From security clearance providers.
- From Occupational Health and other health service providers.
- From Pension administrators and other government departments, for example tax details from HMRC.
- From your Trade Union.
- From the Car Parking Scheme.
- From providers of staff benefits.
- From our landlords or taken using our own CCTV systems.

Back to the top

3. What personal data do we process and why

3.1. Information related to your employment

We use the following information to carry out the contract we have with you, provide you access to business services required for your role and manage our people services processes. We will also use it for our regulatory purposes in our role as a supervisory authority:

- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses.
- Your date of birth, gender and NI number.
- Your photograph.
- A copy of your passport or similar photographic identification and proof of address documents.
- Your electronic signature when you sign off documents.
- Marital status.
- Your next of kin, emergency contacts and their contact information.
- Employment and education history, including your qualifications, job application, employment references, right to work information and details of any criminal convictions that you declare.
- Location of employment (e.g. Wilmslow or regional offices).
- Details of any secondary employment, political declarations, conflict of interest declarations or gift declarations.
- Security clearance details including basic checks and higher security clearance details according to your job.
- Any criminal convictions that you declare to us.
- Your responses to staff surveys if this data is not anonymised.
- Your political declaration forms in line with our policy and procedure regarding party political activities.
- Any content featuring you produced for use on our website, intranet or social media such as videos, authored articles, blog posts and speech transcripts.

Back to the top

3.2. Information related to your salary, pensions and loans

We process this information for the payment of your salary, pension and other employment related benefits. We also process it for the administration of statutory and contractual leave entitlements such as holiday or maternity leave:

- Information about your job role and your employment contract including your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working).

- Details of your time spent working and any overtime, expenses or other payments claimed, including details of any loans such as for travel season tickets.
- Details of any leave including sick leave, holidays, special leave etc.
- Pension details, including membership of both state and occupational pension schemes (current and previous) and your contributions.
- Your bank account details, payroll records and tax status information.
- Trade Union membership for the purpose of the deduction of subscriptions directly from salary.
- Details relating to Maternity, Paternity, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms or matching certificates and any other relevant documentation relating to the nature of the leave you will be taking.

Back to the top

3.3. Information related to your performance and training

We use this information to assess your performance, to conduct pay and grading reviews and to deal with any employer-employee related disputes. We also use it to meet the training and development needs required for your role:

- Information relating to your performance at work e.g. probation reviews, PDRs, promotions.
- Grievance and dignity at work matters and investigations to which you may be a party or witness.
- Disciplinary records and documentation related to any investigations, hearings and warnings or penalties issued.
- Whistleblowing concerns raised by you, or to which you may be a party or witness.
- Information related to your training history and development needs.
- Records of attendance at training courses and some ICO events.
- Leadership development profiles.
- Audio, video and transcriptions from any training sessions, meetings or events you attend that are being recorded.

Back to the top

3.4. Information relating to monitoring

We use this information to assess your compliance with corporate policies and procedures and to ensure the security of our premises, IT systems and employees.

- Information about your access to data held by us for the purposes of criminal enforcement if you are involved with this work.
- Information derived from monitoring IT acceptable use standards.
- Photos and CCTV images.

Back to the top

3.5. Information relating to your health and wellbeing and other special category data

We use the following information to comply with our legal obligations and for equal opportunities monitoring. We also use it to ensure the health, safety and wellbeing of our employees:

- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms, health management questionnaires or fit notes i.e. Statement of Fitness for Work from your GP or hospital.
- Accident records if you have an accident at work.
- Details of any desk audits, access needs or reasonable adjustments.
- Information you have provided regarding Protected Characteristics as defined by the Equality Act and s.75 of the Northern Ireland Act for the purpose of equal opportunities monitoring. This includes racial or ethnic origin, religious beliefs, disability status, and gender identification and may be extended to include other protected characteristics.
- Any information you provide to any of our equality and diversity networks; Access and Inclusion, Women's, Men's, Pride, REACH, Healthy Minds and Menopause.

Back to the top

4. Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful basis for processing your personal data under the UK GDPR:

- Article 6(1)(b) which relates to processing necessary for the performance of a contract.
- Article 6(1)(c) so we can comply with our legal obligations as your employer.
- Article 6(1)(d) to protect your vital interests or those of another person.
- Article 6(1)(e) for the performance of our public task.
- Article 6(1)(f) for the purposes of our legitimate interest.

Where the information we process is special category data, for example your health data, the additional bases for processing that we rely on are:

- Article 9(2)(a) your explicit consent.
- Article 9(2)(b) which relates to carrying out our obligations and exercising our rights in employment and the safeguarding of your fundamental rights.
- Article 9(2)(c) to protect your vital interests or those of another person where you are incapable of giving your consent.
- Article 9(2)(f) for the establishment, exercise or defence of legal claims.
- Article 9(2)(g) – where processing is necessary for reasons of substantial public interest
- Article 9(2)(j) for archiving purposes in the public interest.

In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1 of the DPA 2018. This relates to the processing of special category data for employment purposes. Our Appropriate Policy Document provides further information about this processing.

We process information about staff criminal convictions and offences. The lawful basis we rely on to process this data are:

- Article 6(1)(e) for the performance of our public task. In addition, we rely on the processing condition at Schedule 1 part 2 paragraph 6(2)(a) of the DPA 2018.
- Article 6(1)(b) for the performance of a contract. In addition, we rely on the processing condition at Schedule 1 part 1 paragraph 1 of the DPA 2018.

Our Appropriate Policy Document provides further information about this processing.

Back to the top

5. How long do we keep your personal data

For further information about how long we hold your personal data, see our Retention and Disposal Policy.

Back to the top

6. Data sharing

We have a Personal Data Sharing Policy, which sets out our data sharing rules, to ensure we share personal data lawfully and fairly with other controllers.

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including our data processors, training providers, our solicitors, legal advisors or counsel, government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax and national insurance contributions.

Additionally, we are required under the Public Records Act 1958 (as amended) to transfer records to the National Archives (TNA) for permanent preservation. Some of these records may include the personal data of our current and former employees. Full consideration will be given to Data Protection and Freedom of Information legislation when making decisions about whether such records should be open to the public.

Back to the top

7. Do we use any data processors?

Yes - a list of our data processors can be found at Annex A.

Back to the top

8. Your rights in relation to our processing

As an individual you have certain rights regarding our processing of your personal data, including the right to lodge a complaint with the Information Commissioner as the relevant supervisory authority. For more information on your rights, please see 'Your rights as an individual'.

Back to the top

9. Overseas transfers of your personal data

We don't routinely transfer staff personal data overseas, but when this is necessary, we ensure that we comply with UK GDPR, ensuring appropriate safeguards are in place.

Back to the top

10. Further information

10.1. Personnel files

Both physical and electronic records are held for each member of staff. Data is held securely on ICO systems and at our premises. Some data is held securely with our off-site storage contractor OASIS Group. A link to their privacy notice can be found in Annex A.

You can request your personnel file by contacting People Services or by submitting an access request to accessicoinformation@ico.org.uk. You can also make a verbal request for your information. You will not be able to take away your physical file. Your access request will be handled outside of our normal case management systems with strict restrictions on

access. We will consult internally with members of staff who might hold personal data about you.

Back to the top

10.2. Car park scheme

The car park scheme is operated by staff, though the ICO does process some of the personal information of scheme members to make deductions from your salary. Our facilities department also hold vehicle licence plate details linked to you. These details are deleted when members leave the scheme.

Back to the top

10.3. Staff surveys

We conduct most staff surveys via Microsoft Forms, and all staff can survey colleagues in this way. Staff are advised to pseudonymise surveys by default and to provide sufficient information to colleagues about how their response data will be used.

In addition, Ipsos Karian and Box (IKB) oversee our People Survey and our Pulse Survey tool by acting as our data processor. We share staff names and email addresses with IKB as well as data about our directorates, job roles and reporting lines so they can administer the surveys and report on results. For staff on long term absence, we may share your personal email address so you can receive surveys.

We take steps to ensure these survey responses from staff are pseudonymised. This means that no one at the ICO will be able to link survey responses back to individuals. Participation in most staff surveys is entirely optional.

Survey questions often require quantitative responses; however free text boxes are sometimes included. We advise you not to share identifiable information about yourself in these boxes if you wish to remain anonymous. When appropriate we will also provide additional 'just in time' privacy information regarding specific surveys.

Responses to Health and Wellbeing surveys may be shared with external equality and diversity auditors.

Back to the top

10.4. Customer Surveys

When we send customers the outcome of their complaint, we ask them to complete an optional feedback survey. Responses include their case reference number and rankings relating to the service they received, and their feedback may identify individual members of staff. We use their feedback to help us gauge how well we're handling complaints and to identify opportunities for improvement.

Back to the top

10.5. Whistleblowers

The ICO has a policy and procedure in place to enable its current staff and ex-employees to have an avenue for raising concerns about malpractice. If you wish to raise a concern please refer to the ICO's Whistleblowing policy and procedure. Information in this context is processed by us because it is necessary for our compliance with our legal obligations under the Public Interest Disclosure Act 1998 and The Public Interest Disclosure (Northern Ireland) Order 1998.

Although every effort will be taken to restrict the processing of your personal data and maintain confidentiality whether this is possible will be dependent on the nature of the concern and any resulting investigation.

Back to the top

10.6. Equal opportunities monitoring

Equal opportunities information provided by job applicants is attached to the relevant application on our applicant tracking system Workday when you apply for a role at the ICO.

This information is not made available to any staff outside our recruitment team (including hiring managers) in a way which can identify you. This

information is anonymised after six months and retained for reporting purposes only.

We may periodically participate in external audits to monitor our compliance with the Public Sector Equality Duty, meaning this equality and diversity information may be provided to external auditors. You may also be asked to participate in focus groups or interviews during these audits however participation is not mandatory.

We have a legal obligation to ensure that the intranet and website are accessible in line with the WCAG 2.2 guidelines. We use a third-party, Silktide, to assess the accessibility of our intranet and website. Any personal data and special category data you add to the intranet and website will also therefore be processed by Silktide to ensure that our we are compliant with these guidelines. A link to their privacy notice can be found in Annex A.

We also use Solirius Reply Ltd to carry out accessibility audits to help ensure that the systems and resources we provide to staff meet accessibility standards. A link to their privacy notice can be found in Annex A.

Back to the top

10.7. Equality and diversity networks

Our equality and diversity networks; Access and Inclusion, Women's, Men's, Pride, REACH, Healthy Minds and Menopause help to raise awareness of equality and diversity issues across the ICO and contribute to the development of our internal policies, procedures and practices.

Any information you share with the networks will be treated by them in confidence. Network representatives may signpost you to other ICO staff, for example HR colleagues, or appropriate third-party services. Your information will only be shared by the networks with a third party if you agree to this or it is necessary to protect your vital interests or those of another person.

Back to the top

10.8. Workforce Development and Planning

Our Organisation Development and Capability team uses online learning platforms such as Civil Service Learning to facilitate work related courses. We also use Learning Pool. Links to their privacy notices can be found in Annex A. We will share some information about you with these providers both prior to you joining the ICO and during your employment to ensure you have the necessary access to complete the training required for your role.

We will also routinely share information about you with our other training providers. For example, this will include information such as your name, contact details and job role. When necessary, we will also share information about any dietary or access requirements that you might have when you attend training events.

Optional psychometric testing is available, facilitated by our People Services colleagues. Testing is carried out by Insights Learning and Development Limited, and further information about what personal data you will be required to share is available in their privacy policy. The output of this testing is a Personal Profile report. These reports are treated as confidential and will only be seen by our trained facilitators in People Services and you, unless you choose to share your personal profile more widely.

You can apply to become a Mental Health First Aider and your application form is retained for 3 years. Training is provided by MHFA England, and you will be required to register for training via the MHFA website. For more information on how MHFA will process your personal data please see the MHFA England privacy notice.

Back to the top

10.9. Resources to help with your work

We provide member access to professional bodies and journal subscriptions for you to use as a resource to inform your work. Any personal data we share with these organisations will be for the purpose of providing you with this access. Your use of these resources should only be within the suppliers' terms and conditions and in line with the ICO code of conduct.

The relevant privacy notices for our memberships and subscriptions can be accessed via the following links:

- Association of Computing Machinery.
- Biometrics Institute.
- BSI, BSI Knowledge and Standards development portal.
- Exponential View (Substack).
- Gartner (including GOV.UK Digital Marketplace).
- Rulefinder Data Privacy (aosphere).
- Harvard Business Review (HBR).
- Health Service Journal (Wilmington Healthcare).
- IAPP.
- IEEE.
- JSTOR (Ithaka).
- MLex (LexisNexis).
- Politico.
- Privacy Laws & Business.
- Institute of Regulation.
- Institute of Internal Communication.
- The Information.
- Ipsos Iris.
- DAMA UK.
- MIT Technology Review
- The Economist

Back to the top

10.10. Occupational health

During your employment you may be referred to occupational health following a request to People Services by you or your People manager. This may result in a face-to-face consultation, a telephone appointment with an occupational healthcare professional, or a medical report from a GP or specialist.

We use Optima Health to provide our occupational health service and we may share some information about you with them as part of the referral. You will be asked to provide your consent for any referral and data sharing Optima and a copy of the referral will be shared with you before the appointment.

The information you provide will be held by Optima, who will give us a fit to work certificate or a report with recommendations. A link to their privacy notice can be found in Annex A. Optima is the data controller for the information it generates.

You can also access additional health related services through BUPA Occupational Health Ltd including health checks and screening services as well as eye tests. A link to their privacy notice can be found in Annex A.

Clare and Illingworth also provide eye tests for our employees and will share information with us about your eye examinations.

Back to the top

10.11. Trade Union Membership

The recognised unions at the ICO are the Public and Commercial Services Union (the PCS) and the FDA. The unions are controllers for the personal information connected to your union membership. The ICO holds some union subscription details to process salary deductions for union membership for which you will have given your consent.

Back to the top

10.12. Monitoring of staff

All our ICT systems, EDRM system and the swipe access system for the entry and exit of our premises are auditable and can be monitored, though we don't do so routinely.

We are committed to respecting individual users' reasonable expectations of privacy concerning the use of our ICT systems and equipment. We reserve the right to log and monitor user activity, including email and internet use, to detect and prevent improper use of our systems, in line with our Acceptable Use Policy.

Any targeted monitoring of user activity shall be performed with the approval of People Services, and in compliance with the Data Protection Act 2018.

Back to the top

10.13. Staff involved in criminal enforcement

If you are involved with the process of criminal enforcement - some staff in Legal Services, Intelligence or the Financial Recovery Unit - we monitor and log your access to the information being processed.

Part 3 of the Data Protection Act 2018, which concerns law enforcement processing requires us to keep logs. Section 62 states that these logs must make it possible to establish the identity of the person who consulted the data, the date and time it was consulted and the justification for doing so. Beyond this, the logs must make it possible to establish the identity of the person disclosing the data, the date and time it occurred and the identity of the recipients. These logs are kept to assist with self-monitoring by the ICO, including internal disciplinary proceedings, verifying the lawfulness of the processing, ensuring the integrity and security of personal data, and for the purposes of criminal or regulatory proceedings.

Back to the top

10.14. Financial monitoring

We use an ERP financial accounting system (Workday) to log every financial transaction. This includes any transactions or loans made by or to staff. If an outstanding debt by a member of staff is highlighted via this process, the ICO will use this information to take steps to recover the outstanding amount.

Back to the top

10.15. Security clearance

We conduct basic security checks or advanced checks based on your role in line with the Baseline Personnel Security Standards (BPSS) and the government Security Policy Framework. For temporary staff appointments, BPSS checks are carried out by Alexander Mann Solutions (AMS) on our behalf.

The ICO's security clearance applications are processed by HMRC. Scottish applicants are required to complete a Basic Disclosure check via Disclosure Scotland.

In addition, some staff are required to get Security Clearance, Developed Vetting (DV) or a Counter Terrorist Check (CTC) which is also carried out by HMRC. The outcomes of these checks are stored on our systems.

Back to the top

10.16. Security passes

All staff are all issued with a security pass that displays their name, department, staff reference number and photograph. Staff pass details (names, numbers and photographs) are held on a standalone machine controlled by Facilities and can only be accessed by a restricted number of people. Should you lose your pass you will need to complete a lost security pass form and return it to Facilities. When you leave the ICO your details are deleted as soon as possible from this system.

Back to the top

10.17. Signing in and out of our offices

All staff are required to electronically sign in and out when attending an ICO office. To do this, you must present your security pass at a scanning terminal whenever you enter or exit the building. The scanner records your pass number, which is used to identify you, as well as the office and the date and time you scanned your card. This information is collected for the purpose of generating an accurate roll call report for any ICO office in the event of an evacuation, as well as to identify members of staff present who are designated fire wardens, first aiders, or mental health first aiders.

The information collected will not be used to monitor your office attendance and is anonymised at the end of each week. We use this anonymous data to generate statistical reports to help us better understand office occupancy levels over time.

Back to the top

10.18. CCTV

We operate CCTV at our Wilmslow and Belfast premises to monitor access to our offices. We also operate CCTV inside our Wilmslow premises to monitor access to certain areas of the office. Further information is available in our CCTV policy.

Additionally, staff working in Wilmslow, London, and our other regional offices, may be filmed by CCTV which is owned and operated by the landlords or owners of the buildings in which our offices are situated. The ICO is not the data controller for this information.

Back to the top

10.19. Disclosures in response to information requests

As both a public authority and controller we receive information requests under the Freedom of Information Act (2000) and the UK GDPR and we must consider whether to disclose information about our staff in response to these requests.

We generally disclose employee information only as set out in our Disclosure of ICO employee information policy, which outlines our approach to such requests and what staff can reasonably expect us to disclose about them. While not exhaustive, it provides guidance for staff and request handlers on disclosures under FOI, data protection legislation, and what we proactively publish.

The Information Access Team (IAT) do not typically consult with individuals prior to disclosure, however, they may do so where the information in question is not reasonably expected to be shared. In such instances, they will ensure that any disclosure is appropriately justified, compliant with data protection legislation, and consistent with our internal policies.

Where information can be provided in an anonymised or aggregated format we will establish that ICO employees are not identifiable prior to making a decision on disclosure.

If there are exceptional circumstances where the release of your identity would result in harm to you or others close to you, part five of the

Disclosure of ICO employee information policy explains how to raise such concerns with HR and the IAT. It also sets out how you can submit an individual rights request under the data protection legislation, including your right to object to processing under article 21 of the UK GDPR. An objection to processing can be made at any time, however, you should contact HR and IAT as soon as possible if you need to make us aware of a specific reason why your personal information (for example, your name, place of work and photo) should not be disclosed.

Back to the top

10.20. Requests for references

If you leave, or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference. For example, we may be asked to confirm the dates of your employment or your job role. If you are still employed by us at the time the request for a reference is received, we will discuss this with you before providing this.

Back to the top

10.21. Car Sharing

The ICO Green Group operates a car sharing scheme with the aim of reducing our carbon emissions. If you sign up to this scheme then you will need to provide your name, place of work and some generalised information about your home location and the route you travel to work. Staff are discouraged from sharing their full home address as this information is published to all staff so colleagues interested in car sharing can identify suitable matches. Signing up for the scheme is voluntary and participants can withdraw and delete the information they provided at any time.

Back to the top

10.22. Meetings and events

We use Microsoft Teams to enable online and hybrid meetings and events across the organisation. When needed, recording and transcription will be used, for example:

- to allow colleagues unable to attend to catch up; and
- to enable more detail to be captured.

We ask colleagues to use their judgement prior to using recording or transcription functionality. Not all meetings and events will be suitable for recording or transcription due to the nature of the meeting or sensitivity of the content being discussed. As far as is reasonably possible, we ask all colleagues to give advance notice to attendees of any intention to record or transcribe a meeting or event. Microsoft Teams recordings and transcripts are retained in Teams for 21 days.

Within meetings and events, we may use Slido to create interactive live polls, conduct question and answer exercises or produce quizzes. We will retain the data we collect for up to 12 months to analyse the responses. Use of Slido is not required to attend a meeting or event.

Back to the top

10.23. Booking travel and accommodation

The ICO uses Clarity Travel Ltd to book travel and accommodation. All staff have their own account profile which contains their title, name, and work email address. Staff can add additional personal information to their account profile if they choose, and when necessary to fulfil a required service.

Some staff have permission to make bookings on behalf of colleagues and in limited circumstances, individuals not employed by the ICO. Staff making bookings for individuals not employed by the ICO should provide them with a link to Clarity Travel Limited's privacy policy.

Back to the top

10.24. Cycle to Work Scheme

The ICO offers staff the choice to join the Cycle to Work Scheme and we use Cycle Solutions as our provider. If you sign up for the scheme, you

will provide Cycle Solutions with the following information name, address, telephone number, e-mail address, tax rate, Credit / Debit card details and if required a unique identifier (for example, Payroll Number or National Insurance Number). You will provide this information directly to them and Cycle Solutions will be the data controller for your personal data. Cycle Solutions will then share with the ICO the amount of money that will need to be deducted from your salary.

Back to the top

10.25. Microsoft 365 Copilot

We use Microsoft 365 Copilot (Copilot) to enhance staff productivity and efficiency and for making reasonable adjustments to improve accessibility.

Copilot utilises large language models (LLMs), a type of artificial intelligence (AI) algorithm that uses deep learning techniques to understand, summarise, predict, and generate content.

We use these tools to help summarise information (such as emails, Teams chat messages and meeting transcripts, documents), for example to prepare for meetings, create and format documents, analyse data such as public consultation responses, and generate content such as draft emails or presentations. They also assist with note-taking and idea generation to support efficient communication and decision-making.

Any data, used with Copilot, is stored and stays within our secure UK Microsoft 365 and Azure tenants, and is not used for training foundation models.

We may collect audio and visual recordings, as well as transcripts, of conversations held using Microsoft Teams. The transcription function in Teams allows Copilot to produce some of the outputs referred to above. Recordings and transcripts are automatically deleted after 21 days. All Copilot prompts and responses are deleted after 7 days.

Copilot Memory allows Copilot to remember key factual information about you as a user across conversations to provide more personalised responses. It stores details such as preferences, work context and

recurring topics, which you can view and manage through the settings pane.

No decision affecting ICO staff will be taken based solely on the Copilot output. We will continue to monitor our use of Copilot to review the risks and benefits of this deployment. Any extension of our use will be considered under our risk assessment processes, and this privacy notice will be updated accordingly.

Back to the top

10.26. Assistive technologies

To meet accessibility needs we provide some colleagues with assistive technologies to support them with their work. For example, Livescribe Smartpens to assist with note taking in meetings and training sessions. Users of these technologies are provided specific training covering appropriate use and best practice for handling any personal data recorded with these technologies.

Back to the top

11. Annexes

Annex A - data processors

Data processors are third parties who provide certain parts of our staff services for us. We have contracts in place with them, and they cannot do anything with your personal information unless we have instructed them to do so. Our data processors are listed below.

Data Processor	**Purpose**	**Privacy Notice**
Vacancy Filler Ltd.	Applicant tracking system for recruitment	Vacancy Filler
MyCSP	For administering Civil Service Pensions	Civil Service Pension Scheme

Data Processor	Purpose	Privacy Notice
Condeco	Meeting Room bookings	Condeco
CEB	Provider of online tests	CEB
Hays Specialist Recruitment Ltd (t/a Hays Executive)	Recruitment agency used for senior vacancies	Hays Recruitment
BHSF Employee Benefits Ltd	Staff cash health provider	BHSF
Legal and General	Partnership pension provider	Legal and General
Bupa	Private medical care	Bupa
CVS	Childcare voucher provider	CVS
Salary Extras	Cycle to work scheme	Salary Extras
HMRC	Security clearance applications, Data disposal services	HMRC
Forbes	Legal services provider	Forbes Solicitors
Civil Service Learning	Training provider	Civil Service Learning
Learning Pool	Training provider	Learning Pool
The Myers-Briggs Company	Training provider	The Myers-Briggs Company
Omniplex Learning	Training provider	Omniplex Learning

Data Processor	Purpose	Privacy Notice
OASIS Group	Document Storage	OASIS Group
Snap Surveys	Staff Surveys	Snap Surveys
Canon	Printing services	Canon
Halo	IT ticketing software	Halo ITSM
TMSDI	TMS profiles	tmsdi
Revealing Reality	Research Function Development	Revealing Reality
Clear Company	Equality and Diversity auditors	Clear Company
Microsoft	MMD and software	Microsoft
XBP Europe Ltd	Digital mailroom	XBP Global
Skillsoft	e-Learning provider	Skillsoft
Twilio	SendGrid Email API	Twilio
Palo Alto Networks	Proxy and VPN services	Palo Alto Networks
Comaea	Training provider	Comaea
Silktide	Website and intranet accessibility	Silktide
Workday	Workforce Management software	Workday
Slido	Event management	Slido

Data Processor	Purpose	Privacy Notice
Symbiant	Audit Software	Symbiant
Kainos	Provider of Application Management Services for Workday	Kainos
The Oakland Group	Partner in developing the ICO Enterprise Data Strategy	The Oakland Group
Canva	Branded content design for internal communications	Canva
Alexander Mann Solutions (AMS)	Baseline Personnel Security Standards checks for temporary staff appointments	AMS
Ipsos Karian and Box	Administration of People Survey	Ipsos Karian and Box
Clarity Travel Limited	Booking of travel, accommodation, car hire, and meeting rooms	Clarity Travel Limited
Nasstar	Workforce management solution using the Calabrio platform	Nasstar Calabrio
Personal Audit Systems Ltd	To generate tax forms relating to expenses and benefits	P11D Organiser

Data Processor	Purpose	Privacy Notice
Azure Consulting	Coaching and Leadership Development services.	N/A
Delib Ltd	Consultations and surveys using the Citizen Space platform	Delib
Figma	Tool for user centred design	Figma
BiP Solutions Limited	Procurement software	Privacy Policy - BiP Solutions
CapGemini	Enterprise Data Strategy development partner	N/A
Gurock Software GmbH	Provider of TestRail test management tool	Gurock Legal - An Idera company
Articulate Global	E-learning platform	Privacy Notice | Articulate
Ardoq	Enterprise architecture software	Privacy Notice | Ardoq
ABM Intelligence Limited T/a Altia	Altia transcription software for investigation interviews	Privacy Policy - Altia Intel
Gatenby Sanderson	Leadership development programme	Privacy Statement - GatenbySanderson
Atlassian	Project management software	Privacy Policy | Atlassian
Solirius Reply Ltd	Undertakes accessibility audits	Privacy Policy | Solirius

Data Processor	Purpose	Privacy Notice
EY	Training materials	Privacy statement | EY - UK
Nexer Digital	Website support and development	Privacy policy - Nexer Digital
Squiz Pty Ltd	Website search engine provider	Privacy policy | Squiz
RedQuadrant Ltd	Systems thinking consultant	RedQuadrant website RedQuadrant Ltd - Privacy Notice
Phoenix Software	Microsoft managed services	Data Protection | Phoenix Software
LinkedIn	Talent recruitment / Corporate Communications	LinkedIn Privacy Policy
Azeus	Provider of Convene board management software used for board, executive, and senior leadership meetings	Convene's Privacy Policy
The Institute of Customer Service	Customer survey	Data Protection Policy ⋆ Institute of Customer Service
Wubbleyou	Data Protection Essentials platform provider	Wubbleyou — Privacy policy
Language Line	Interpreting service	LanguageLine UK | Data Processing

Back to the top

Version history

Version	Changes Made	Date	Made by
1.0	First Published	31/04/2019	Steven Johnston
1.1	Addition of version history control. Update to Resources to help with your work.	10/06/2021	Steven Johnston
1.2	References to GDPR changed to UK GDPR.	14/06/2021	Steven Johnston
1.3	MHFA Mental Health First Aiders	10/08/2021	Tiffany Higgins
1.4	Addition of leadership development profiles. TMSDI added to list of processors.	26/08/2021	Steven Johnston
1.5	Addition of Revealing Reality to list of data processors.	06/12/2021	Steven Johnston
1.6	Addition of photograph in information related to employment section	10/01/2022	Simon Lochery
1.7	Added link to Harvard Business Review Privacy Notice	12/01/2022	Ben Cudbertson

1.8	Added link to MIT Technology Review Privacy Notice	21/01/2022	Ben Cudbertson
1.9	Added links to Association of Computing Machinery and International Institute of Forecasters Privacy Notices.	26/01/2022	Ben Cudbertson
1.10	Added information about external equality and diversity audits.	31/01/2022	Ben Cudbertson
1.11	Added link to the Politico privacy notice.	01/02/2022	Simon Lochery
1.12	Added link to JSTOR privacy notice.	11/03/2022	Simon Lochery
1.13	Added reference to Exponential View under Resources to help with your work.	14/03/2022	Simon Lochery
1.14	Explicit consent added as a processing condition for special category data, addition of Intranet in 'Information related to your employment'.	14/04/2022	Steven Johnston
1.15	Addition of Exela to Annex A.	25/04/2022	Steven Johnston

1.16	Addition of Skillsoft to Annex A.	29/04/2022	Ben Cudbertson
1.17	Updates to Disclosures in response to information requests and staff surveys content. Removed all references to BMG Research. Addition of FSP Consulting Services to Annex A.	04/05/2022	Steven Johnston
1.18	Addition of Twilio to Annex A.	13/07/2022	Steven Johnston
1.19	Added link to World Economic Forum – Strategic Intelligence privacy notice	19/08/2022	Simon Lochery
1.20	Addition of Palo Alto Networks to Annex A	30/09/2022	Steven Johnston
2.0	Review and transferred to new corporate template.	12/12/2022	Steven Johnston
2.1	Section 10.8: Amendments to names of links to third party privacy notices. Addition of privacy notice links for Gartner, Gov.uk Digital Marketplace, and International Data Privacy Law.	19/12/2022	Simon Lochery

	Removal of link to MIT Technology Review as no subscription taken out.		
2.2	Added Comaea to Annex A.	09/02/2023	Ben Cudbertson
2.3	Updated section 10.5 to include website and intranet accessibility. Added Silktide to Annex A.	02/03/2023	Ben Cudbertson
2.4	Addition of Workday to Annex A. Addition of electronic signature to 3.1.	12/05/2023	Steven Johnston
2.5	Addition of link to Global Data Privacy Laws (Aosphere) privacy statement at 10.8. Annex A amended to include data disposal services for HMRC.	05/06/2023	Simon Lochery
2.6	Update to 10.17 following publication of Employee Information Disclosure Policy	05/06/2023	Steven Johnston
2.7	Removal of all references to Health Management Limited as occupational health provider. Update to 10.9 to reflect BHSF now	20/06/2023	Steven Johnston

	occupational health provider.		
2.8	Addition of link to Privacy Laws & Business privacy policy at 10.8.	13/07/2023	Simon Lochery
2.9	Addition of section 10.20. Addition of Slido as a data processor.	17/07/2023	Ben Cudbertson
2.10	Addition of Symbiant as data processor in Annex A.	31/07/2023	Steven Johnston
2.11	Addition of paragraph about Insights Discovery in 10.7	22/08/2023	Steven Johnston
2.12	Link to Politico privacy notice amended at 10.8.	23/08/2023	Simon Lochery
2.13	Addition of Kainos as data processor in Annex A	22/09/2023	Simon Lochery
2.14	Addition of The Oakland Group to Annex A.	23/10/2023	Steven Johnston
2.15	Formatting changes made to meet accessibility requirements	27/10/2023	Ben Cudbertson
2.16	Addition of section 10.4 Customer surveys.	31/10/2023	Simon Lochery

	Section 10 renumbered.		
2.17	Addition of Canva to Annex A.	04/12/2023	Steven Johnston
2.18	6.1 updated to include solicitors, legal advisors and counsel after procurement of DAC Beechcroft for the provision of legal services.	03/01/2024	Steven Johnston
2.19	Link to the Institute of Regulation privacy notice added to section 10.9	25/01/2024	Simon Lochery
2.20	Addition of transcriptions and meetings or events to section 3.3. OASIS Group added to 10.1 and Annexe A for document storage services. References to Restore removed.	31/01/2024	Steven Johnston
3.0	IM&C Service annual review, no changes made.	27/02/2024	Steven Johnston
3.1	Alexander Mann solutions added to section 10.5 for BPSS checks and Annex A.	18/03/2024	Simon Lochery
3.2	Minor changes to section 10.17 CCTV.	10/04/2024	Simon Lochery
3.3	Update to 10.3 to reference Ipsos Karian and Box. Addition of IKB to Annex A.	10/04/2024	Steven Johnston

3.4	Addition of section 10.22 and added Agiito to Annex A.	18/04/2024	Simon Lochery
3.5	Nasstar, and reference to Calabrio, added to Annex A	16/05/2024	Simon Lochery
3.6	Personal Audit Systems Ltd, and reference to P11D Organiser added to Annex A	07/06/2024	Simon Lochery
3.7	Addition of Azure consulting to Annex A	10/06/2024	Steven Johnston
3.8	Addition of Institute of Internal Communication to 10.9	17/07/2024	Caroline Browne
3.9	Section 10.21 amended to account for use of Slido at both internal meetings and events.	31/07/2024	Simon Lochery
3.10	Alexander Mann solutions removed from section 10.5 for BPSS checks and from Annex A	09/08/2024	Simon Lochery
3.11	Alexander Mann Solutions reinstated at section 10.5 and Annex A. Added Delib Ltd, provider of the Citizen Space platform, to Annex A. Added Figma to Annex A.	02/09/2024	Simon Lochery
3.12	BiP Solutions, provide of Delta, added to Annex A.	08/10/2024	Caroline Browne

3.13	Reference to Minfo removed from Security Passes section.	18/10/2024	Simon Lochery
3.14	10.3 updated with more info about using Microsoft Forms for surveys.	21/10/2024	Steven Johnston
3.15	Section added at 10.17 for signing in at offices.	06/11/2024	Simon Lochery
3.16	Addition of CapGemini to Annex A.	27/11/2024	Steven Johnston
3.17	Addition of The Information to 10.9	05/12/2024	Caroline Browne
3.18	Addition of Ipsos Iris to 10.9	05/02/2025	Simon Lochery
3.19	Addition of Gurock Software GmbH to annex A	13/02/2025	Simon Lochery
3.20	Section 10.22 updated to include use of recording and transcription in Microsoft Teams and the Microsoft 365 copilot pilot phase	13/03/2025	Simon Lochery
3.21	Addition of Articulate Global to annex A	27/03/2025	Caroline Browne
3.22	3.33 Updated with information about the recording of attendance of training courses and ICO events	10/04/2025	Caroline Browne
3.23	Section 10.24 added to include information about the Cycle to Work Scheme	29/04/2025	Caroline Browne
3.24	Ardoq added to data processors in Annex A	07/05/2025	Simon Lochery

3.25	ABM Intelligence Limited T/a Altia added to list of data processors	24/06/2025	Steven Johnston
3.26	Addition of Mental Health First Aiders in section 10.17	07/07/2025	Simon Lochery
3.27	Addition of Gatenby Sanderson in Annex A	11/07/2025	Steven Johnston
3.28	Addition of Atlassian in Annex A	23/07/2025	Caroline Browne
3.29	Addition of Phoenix Software to Annex A	10/08/2025	Steven Johnston
3.30	Removed Microsoft 365 Copilot content from 10.22. Added section 10.25 Microsoft 365 Copilot (pilot phase) with updated content following expansion of pilot phase.	19/08/2025	Steven Johnston
3.31	Addition of Solirius and EY to annex A.	22/08/2025	Simon Lochery
3.32	Paragraph added to section 10.6 about use of Solirius Ltd. Addition of Nexer Digital to annex A	28/08/2025	Simon Lochery
3.33	Addition of Squiz pty Ltd to annex A	15/09/2025	Caroline Browne
3.34	Addition of RedQuadrant Ltd to annex A	30/09/2025	Simon Lochery
3.35	Addition of section 10.26	14/10/2025	Steven Johnston
3.36	DAMA UK added to section 10.9.	24/11/2025	Simon Lochery

	Reference to 'Solirius Ltd' in main body of document changed to 'Solirius Reply Ltd'.		
3.37	References to Agiito replaced with Clarity Travel Limited in section 10.23 and in annex A.	19/12/2025	Simon Lochery
3.38	Policy moved to new corporate template. Minor amendment to DPO paragraph in section 1. Minor content, format and grammar changes throughout to update and align with ICO style guide.	02/03/2026	Steven Johnston
3.39	Revised content in section 10.25	12/03/2026	Steven Johnston
3.40	Added Azeus to the list of processors in Annex A	27/03/2026	Simon Lochery
3.41	Amendments to Annex Addition of, Omniplex Learning, Wubbleyou, Language Line, Update Exela Technologies to XBP Europe Ltd Removal of FSP Consulting Services Limited, Wiley, Brightwave, CIPHR and Little Fish	04/06/2026	Lubna Begum
3:42	Section 10.6 updated from WCAG 2.1 to WCAG 2.2. MHFA England privacy policy link corrected. Section 10.9 updated from Global Data Privacy Laws	09/06/2026	Lubna Begum

	(Aosphere) to Rulefinder Data Privacy (aosphere). Section 10.9 - Removed International Data Privacy Law (Oxford University Press), International Institute of Forecasters, World Economic Forum – Strategic Intelligence Section 10.9 - Added MIT Technology Review and The Economist Section 10.10 • Updated references from HR to People Services. • Reference to BHSF amended to Optima Health. • Added statement: "Optima and a copy of the referral will be shared with you before the appointment." Section 10.12 • Updated to include a paragraph regarding staff monitoring in line with the Acceptable Use Policy. Section 10.14 • Updated to include ERP as the financial accounting system. • Reference to Microsoft Dynamics GP amended to Workday. Section 10.19 • Apart from the first paragraph, the entire section was deleted and replaced with a new section.		

Back to the top