Staff Privacy Notice

Document Name	Staff Privacy Notice
Author/Owner (name and job title)	Steven Johnston, Team Manager, Information Management
Department/Team	Information Management
Document Status (draft, published or superseded)	Published
Version Number	v1.27
Release Date	31/04/2019
Approver (if applicable)	Head of Internal Policy Advice
Review Date	31/01/2022
Distribution (internal or external)	External

Staff Privacy Notice

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. Details of our Data Protection Officer can be found here.

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.

In this notice

How do we get your information

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 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.
- CCTV images from our landlords or taken using our own CCTV systems.

What personal data we process and why

We process the following categories of personal data:

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 human resources processes. We will also use it for our regulatory purposes in our role as a supervisory authority and to fulfil our role of promoting openness by public bodies and data privacy for individuals.

- 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 / or proof of address 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 form 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.

Information related to your salary, pension 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).
- 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/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking.

Information relating 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/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.
- Leadership development profiles (360, TMS)
- Audio and video from any training sessions you attend that are being recorded.

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.

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; Women and Allies, Pride, REACH, Healthy Minds and Access Inclusion.

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) in order 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.

Special category data

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 defense 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.

Criminal convictions and offences

We process information about staff criminal convictions and offences. The lawful basis we rely 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.

How long we keep your personal data

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

Data Sharing

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, 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.

Do we use any data processors?

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

Your rights in relation to this processing

As an individual you have certain rights regarding our processing of your personal data, including a 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'.

Overseas transfers of personal data

We don't routinely transfer staff personal data overseas but when this is necessary we ensure that we have appropriate safeguards in place.

Further information

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 Restore PLC. A link to their privacy notice can be found in Annex A.

You can request your personnel file by emailing the HRteam 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 cases management systems with restricted access. We will consult internally with members of staff who might hold personal data about you.

Car park scheme

The car park scheme is operated by staff, though the ICO does process some of the personal information of scheme members in order 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.

Staff surveys

We conduct most staff surveys via the cloud based platforms Snap Surveys and Pulse 360. Any data collected is stored on UK servers. A link to their privacy notices can be found in Annex A.

We take steps to ensure responses from staff are pseudonymised. This means that no one at the ICO will be able to link survey responses to

particular individuals. Participation in most staff surveys is entirely optional.

Survey questions often require quantitative responses, however free text boxes are sometimes included. We would 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 provided to external equality and diversity auditors.

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 'Speak up' - 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.

Equal opportunities monitoring

Equal opportunities information provided by job applicants is attached to the relevant application on our applicant tracking system Vacancy Filler when you apply for a role at the ICO. A link to their privacy notice can be found in Annex A.

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, therefore this equality and diversity information may be provided to external auditors. You may also be asked to participate in focus groups or interviews during the course of these audits, however participation is not mandatory. A link to the auditor's Privacy Notice can be found in Annex A.

Equality and diversity networks

Our equality and diversity networks; Women and Allies, Pride, REACH, Healthy Minds and Access Inclusion 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.

Workforce Development and Planning

Our Workforce and Development and Planning department use online learning platforms such as Civil Service Learning for the facilitation of its 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 training required for your role.

We will also share information about you with our 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.

Application forms to become a Mental Health First Aider are retained by the team for 3 years. Training is provided by MHFA England and staff are 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 policy.

Resources to help with your work

We provide access to memberships to professional bodies and journal subscriptions for the use as a resource to help you with your work. Any personal information shared with these organisations will be used to allow you to use those resources. The use of the resources should only be

within the suppliers' terms and conditions and in line with code of conduct.

Our memberships and subscriptions privacy notices can be accessed via the following links:

Biometrics Institute

BSI, BSOL and Standards development portal

Health Service Journal

IAPP

IEEE

MLex (LexisNexis)

Harvard Business Review (HBR)

MIT Technology Review

Association of Computing Machinery

International Institute of Forecasters

Politico

JSTOR

Exponential View

Occupational health

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

We use Health Management Limited (HML) to provide our occupational health service. The information you provide will be held by HML, 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.

HML act as our data processor in respect of our historic records that have not been used in relation to new referrals. In respect of new referrals which require HML to determine the means and purposes of processing

HML is the data controller and the ICO is the controller for the information it generates and receives from HML in relation to referrals.

BUPA Occupational Health Ltd also provides health checks and screening service and eye tests. A link to their privacy notice can be found in Annex A.

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

Trade Union Membership

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

Monitoring of staff

All of 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. However, we reserve the right to log and monitor such use in line with our Acceptable Use Policy.

Any targeted monitoring of staff will take place within the context of our disciplinary procedures.

Staff involved in criminal enforcement

If you are involved with the process of criminal enforcement - some staff in Legal, 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 that 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 will be 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.

Financial monitoring

We use a financial accounting system (Microsoft Dynamics GP) 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.

Security clearance

Basic security checks and / or advanced checks based on your role in line with the Baseline Personnel Security Standards and the government Security Policy Framework are carried out by HMRC 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 outcome of these checks are stored on our systems.

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. Photographs are uploaded to Minfo by HR staff. 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.

CCTV

We 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, regional and London 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.

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 will normally disclose work-related information about staff in a public-facing role. We may also disclose information about staff members whose work is purely administrative if their names are routinely sent out externally.

It is less likely that information about those who do not deal directly with the public in an operational capacity will be disclosed. The Executive Team and the Senior Leadership Team will have more information disclosed about them, such as photographs and biographical detail, due to their position at the ICO.

We will consider withholding information if we think that it will prejudice our regulatory role or the rights and safety of our staff, irrespective of grade or position.

The type of information you can expect we will routinely disclose is as follows:

- Name and work contact details.
- Pay bands (not your exact salary).
- How long you have worked at the ICO, your current role, any previous roles or secondments and what your role involves.
- Your position in the corporate structure.
- Business related entries in your diary/calendar.
- Summaries of expense claims without details of where you stayed, where you ate or your itinerary.
- Any work related training at the ICO.
- Any work related opinions or conversations, for example case notes, emails or Teams instant messages.

The list above does not include every area where we might disclose information about you. The type of information provided will only concern your professional life at the ICO. We will not disclose non-work related personal or special category data.

When we are asked to disclose diary or calendar information due consideration will be given to the safety of our staff. Where this information is requested outside of an FOI request our staff are advised to consult with their manager before sharing information about a staff member, especially when it concerns movements or whereabouts.

We will consult with you prior to deciding whether to disclose any information that we consider would not be within your reasonable expectations.

Before you begin working at the ICO, contact HR if you need to make us aware of a specific reason why your information cannot be provided as part of a disclosure. At any later point, if you have any concerns about information being released you need to inform us of this fact.

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.

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. The information will be kept for 12 months after the entry is last modified.

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**
Capita Business	Provider of payroll services	Capita

Services Ltd		
Vacancy Filler Ltd.	Applicant tracking system for recruitment	Vacancy Filler
Littlefish	Provider of our managed IT service for our IT infrastructure	Littlefish
MyCSP	For administering Civil Service Pensions	Civil Service Pension Scheme
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
Health Management Ltd	Occupational Health provider	Health Management
BHSF Employee Benefits Ltd	Staff cash health plan	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	HMRC
Forbes	Legal services provider	Forbes Solicitors
CIPHR	HR records and database system	CIPHR
Civil Service	Training	Civil Service Learning

Learning	provider	
Learning Pool	Training provider	Learning Pool
Brightwave	Training provider	Brightwave
Restore Plc	Document Storage	Restore
Snap Surveys	Staff Surveys	Snap Surveys
Wiley	DiSC assessments	Wiley
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
Exela Technologies	Digital mailroom	Exela
Skillsoft	e-Learning provider	Skillsoft
FSP Consulting Services Limited	Pulse 360	FSP

Version History

Version	Date	Amended by	Comments
v1.11	10/06/2021	Steven Johnston	Addition of version history control. Update to Resources to help with your work.
v1.12	14/06/2021	Steven Johnston	References to GDPR changed to UK GDPR.
v1.13	10/08/2021	Tiffany Higgins	MHFA Mental Health First Aiders
v1.14	26/08/2021	Steven Johnston	Addition of leadership development profiles. TMSDI added to list of processors.

v1.15	06/12/2021	Steven Johnston	Addition of Revealing Reality to list of data processors.
v1.16	10/01/2022	Simon Lochery	Addition of photograph in information related to employment section
V1.17	12/01/2022	Ben Cudbertson	Added link to Harvard Business Review Privacy Notice
V1.18	21/01/2022	Ben Cudbertson	Added link to MIT Technology Review Privacy Notice
V1.19	26/01/2022	Ben Cudbertson	Added links to Association of Computing Machinery and International Institute of Forecasters Privacy Notices.
V1.20	31/01/2022	Ben Cudbertson	Added information about external equality and diversity audits.
V1.21	01/02/2022	Simon Lochery	Added link to the Politico privacy notice.
V1.22	11/03/2022	Simon Lochery	Added link to JSTOR privacy notice.
V1.23	14/03/2022	Simon Lochery	Added reference to Exponential View under Resources to help with your work.
V1.24	14/04/2022	Steven Johnston	Explicit consent added as a processing condition for special category data, addition of Intranet in 'Information related to your employment'.
V1.25	25/04/2022	Steven Johnston	Addition of Exela to Annex A.
V1.26	29/04/2022	Ben Cudbertson	Addition of Skillsoft to Annex A.
V1.27	04/05/2022	Steven Johnston	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.