Data Protection Policy

Document name	Data Protection Policy
Version number	3.0
Status	Published
Department or Team	Information Management & Compliance
Relevant policies	Appropriate Policy Document - Our Processing of Special Categories of Personal Data and Criminal Offence Data Appropriate Policy Document - Law Enforcement Processing
Distribution	Internal and External
Author/Owner	Information Management & Compliance
Approved by	Data Protection Officer (DPO)
Date of sign off	22/09/2021
Review by	31/01/2025
Security classification	Official

Key messages

The purpose of this document is to outline:

- How the ICO will ensure compliance with the UK GDPR and Data Protection Act 2018.

- Explain the roles and responsibilities relevant to internal compliance.
- How compliance with this policy will be monitored.

Does this policy relate to me?

This policy applies to all the processing of personal data carried out by the ICO including processing carried out by joint controllers, contractors, and processors.

Table of contents

1. Introduction

1.1. This policy provides a framework for ensuring that the ICO meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

1.2. The ICO complies with data protection legislation guided by the six data protection principles.

In summary, they require that personal data is:

- processed fairly, lawfully and in a transparent manner.
- used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.
- adequate, relevant, and limited to what is necessary.
- accurate and, where necessary, up to date.
- not kept for longer than necessary; and
- kept safe and secure.

1.3. In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

1.4. Our staff have access to a number of policies, operational procedures and guidance to give them appropriate direction on the application of the data protection legislation, this includes over-arching documents such as;

- Information Management Policy
- Retention and Disposal Schedule
- Appropriate Policy Document - Our Processing of Special Categories of Personal Data and Criminal Offence Data
- Appropriate Policy Document - Law Enforcement Processing

Back to Top

2. Information Covered by Data Protection Legislation

2.1. The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

2.2. Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

2.3. Some personal data is more sensitive and is afforded more protection, this is information related to:

- Race or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data;
- Biometric ID data;
- Health data;
- Sexual life and/or sexual orientation; and
- Criminal data (convictions and offences)

Back to Top

3. Our Commitment

3.1. The ICO is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about customers, staff or those who work or interact with us.

3.2. **Information Asset Owners** – we assign an Information Asset Owner (IAO) to each information asset throughout the organisation,

who together with a network of teams and staff with information management responsibilities aid the ICO in managing personal data and its associated risks.

3.3. **Privacy Notices** - we publish a privacy notice on our website and provide timely notices where this is required. We track and make available any changes in our privacy notice. We also publish a staff privacy notice and keep it up to date.

3.4. **Training** - we require all staff to undertake mandatory training on information governance and security which they re-take every year. In addition, all staff are required to attend a more detailed data protection training module as part of their induction.

3.5. **Breaches** - we consider personal data breach incidents and have a reporting mechanism that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA. We take appropriate action to make data subjects aware if needed.

3.6. **Information Rights** - we have a dedicated team and clear processes to handle subject access requests and other information rights requests.

3.7. **Data Protection by Design and Default** - we have a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and processes to assist staff in ensuring compliance and privacy by design is integral part to any product, project or service we offer.

3.8. **Records of Processing Activities (ROPAs)** - we record our processing activities and publish our safeguards policy on law enforcement processing and processing of special category data.

3.9. **Policies and Procedures** - we produce policies and guidance on information management and compliance that we communicate to staff.

3.10. **Communications** - We have a clear communication plan which seeks to embed a culture of privacy and risk orientation.

3.11. **Contracts** - Our Commercial legal department oversee that our contracts are compliant with UK GDPR.

Back to Top

4. Roles and Responsibilities

4.1. We have an established Information Risk Management Network that ensures the risk to personal data across the ICO is identified and appropriately managed. This network's detailed roles and responsibilities comprises of the below.

4.1.1. **Risk and Governance Board (RGB)**. RGB is responsible for the overview and scrutiny of information governance (IG) arrangements and for making recommendations to the Senior Information Risk Owner (SIRO) on information governance with data protection and compliance decisions.

4.1.2. **Data Protection Officer (DPO)**. The ICO Data Protection Officer (DPO) is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR and making recommendations to improve compliance. The ICO DPO is Louise Byers, and she can be contacted at DPO@ico.org.uk

4.1.3. **Senior Information Risk Owner (SIRO)**. The SIRO owns the overall risk arising from the processing personal data by

the ICO. Our SIRO is the Deputy Chief Executive and Chief Operating Officer of the ICO, Paul Arnold.

4.2. **Other roles**. Specific roles are assigned throughout our corporate hierarchy to manage personal data we process and the associated risks in terms of responsibilities, decision making and monitoring compliance.

4.2.1. **Information Asset Owners (IAOs).** IAOs have local responsibility for data protection compliance in their area/directorate.

4.2.2. **Information Asset Managers (IAMs).** IAMs support IAOs in complying with their duties regarding the processing of personal data.

4.2.3. **Local Information Management Officers (LIMOs)**. LIMOs advise their departments on information management and carry out specified information management tasks.

4.2.4. A number of teams are responsible for issuing, reviewing and communicating corporate information management policies and procedures. The teams also advise on compliance with data protection and implement IT solutions to ensure we take a privacy by design approach.

Back to Top

5. Monitoring

5.1. Compliance with this policy will be monitored via the DPO and the responsible teams reporting to RGB and Audit Committee.

Back to Top

6. Further Information

6.1. Our corporate standards and policies are available via the following links:

Policies and procedures

Information rights request

Privacy notice

Back to Top

Feedback on this document

If you have any feedback on this document, please fill in this feedback form.

Back to Top

Version history

Version	Changes made	Date	Made by
0.1	Document created	15/07/2020	Iman El Mehdawy
1.0	First release	15/09/2020	Iman El Mehdawy
1.1	Content moved to new template, minor formatting changes	06/09/2022	Ben Cudbertson

Version	Changes made	Date	Made by
2.0	Reviewed, no change	30/01/2023	Iman El Mehdawy
2.1	Formatting changes to meet accessibility requirements	26/04/2023	Ben Cudbertson
3.0	Reviewed, no change	30/01/2024	Rosie Simpson

Back to Top

Annexes

Annex A – Glossary

Personal data. Any information relating to an identifiable living individual who can be identified from that data or from that data and other data. This includes not just being identified by name but also by any other identifier such as ID number, location data or online identifier, or being singled out by any factors specific to the physical, physiological, genetic, mental, cultural or social identity of the individual.

Processing. Anything that is done with personal data, including collection, storage, use, disclosure, and deletion.

Special category personal data. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health or data concerning an individual's sex life or sexual orientation.

Controller. The organisation (or individual) which, either alone or jointly with another organisation (or individual) decides why and how to process personal data. The Controller is responsible for compliance with the DPA and GDPR.

Personal Data Breach. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored, or otherwise processed.

Pseudonymisation. The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.