Data Protection Policy

Policy statement

{NAME OF ORGANISATION} (hereafter we/us/our/the organisation) is committed to ensuring that all personal data we process, including that of colleagues and customers, is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "DP legislation").

Negligent or malicious non-compliance with this policy may be dealt with through the disciplinary process.

Document control

Document title:
Version number:
Author:
Owner:
Approval Date:
Review Date:
Version history:

Related documents

- Special Category Data Protection Policy
- Information Security Policy
- Information Security Incident Procedure
- Information Asset Register
- Record of Processing Activity

This document includes links to guidance published by the UK Information Commissioner's Office (ICO) and by the European Data Protection Board (EDPB).

Responsibilities

- The **Chief Executive** has overall responsibility for ensuring our compliance with this policy and with DP legislation;
- {Some organisations may choose to designate a **Senior Information Risk Owner** at executive level with oversight of data protection and other aspects of information governance}.
- The **Data Protection Lead** (DP Lead) has day-to-day responsibility for monitoring compliance with this policy, advising the organisation on data protection matters and for receiving reports of personal data incidents for escalation as appropriate. {*This assumes that the organisation does not meet the criteria under GDPR for mandatory designation of a Data Protection Officer. Should that be the case, replace all references to Data Protection Lead with Data Protection Officer.*}
- **Heads of Department** are responsible for ensuring that all systems, processes, records and datasets within their business area are compliant with this policy and with DP legislation; for assisting the DP Lead in their duties through providing all appropriate information and support; for ensuring that their staff are aware of their data protection responsibilities; and consulting the DP Lead on new developments or issues affecting the use of personal data in the organisation; for ensuring Data Protection Impact Assessments are conducted as appropriate on data processing activities in their business area, drawing on advice from the DP Lead. {Some organisations may choose to designate a specific role of **Information Asset Owner** at senior management level with accountability to the Senior Information Risk Owner.}
- **All colleagues** are responsible for understanding and complying with relevant policies and procedures for handling personal data appropriate to their role, and for immediately reporting any event or breach affecting personal data held by the organisation.

The data protection principles

We will at all times comply with the data protection principles in respect of all personal data processed by us. This includes personal data relating to colleagues, volunteers, service users, customers, potential customers and business contacts.

All personal data will be:

See also ICO guidance on the data protection principles.

Governance of data protection

The organisation will maintain oversight and transparency in the management of personal data. We will meet our accountability duties through the maintenance of the following record-keeping systems:

- Up-to-date **privacy notice information** for colleagues, customers and service users;
- A **Record of Processing Activity (ROPA)** describing the content, purpose, controls and accountability for each data system or set of records holding personal data within the organisation (See Excel workbook ***Data Protection trackers***);
- A **log of information security incidents** impacting on personal data held by the organisation. (See Excel workbook ***Data Protection trackers***)

Our Records of Processing Activities, under Article 30 of GDPR, will include all the information required to comply with paragraph 41 of Schedule 1 of DPA 2018. (See also the ***Special Category Data Policy***).

See also: ICO guidance on the right to be informed, on required documentation

Data Protection by Design

We will apply Data Protection by Design principles to new systems and business processes through consulting the Data Protection Lead on the acquisition and development of new information systems and on proposals for significant new business processes and change.

Criteria for development and acquisition of IT systems will include data protection compliance requirements for security and functionality.

As appropriate, the Data Protection Lead may advise the relevant head of Department to complete a Data Protection Impact Assessment in line with the organisation template and guidance from the Information Commissioner's Office.

All contracts with organisations who are processing personal data on behalf of the organisation (**data processors**) will have GDPR-compliant contract clauses and be subject to appropriate levels of review and oversight. This will clearly set out expectations for how external contractors and suppliers must handle personal data relating to our colleagues, contacts and customers.

See also: See ICO guidance on accountability requirements, and EDPB guidelines on Data protection impact assessments and high-risk processing.

Data minimisation and accuracy

All colleagues must only record appropriate, accurate and relevant personal data in the course of their duties. This personal data must only be held on authorised forms and information systems – they must not be held on personal notes or devices.

Heads of Department must ensure that within their area of responsibility, IT systems, forms and templates are kept under review to ensure that by design they only capture the minimum personal data necessary for the business activity.

See also: ICO guidance on data minimisation and accuracy.

Retention of personal data

Personal data must not be retained for longer than is necessary for the purpose for which it was gathered. Heads of Department are responsible for ensuring that the Records Retention Schedule is applied to all records, data and documents holding personal data within their business area, by having regular or automated deletion or destruction of personal data in systems, paper files and on network folders. All documents and media containing personal data should be disposed of securely as confidential waste.

See also: relevant ICO Guidance.

Individual rights

We will ensure that individuals' rights over their personal data are respected. These rights include:

All requests made by individuals (colleagues, contacts or customers/service users) relating to their personal data rights must immediately be forwarded to the Data Protection Lead who will ensure that appropriate actions are taken, and a response issued without undue delay and at least within one month.

See also: Relevant ICO guidance and EDPB guidelines on Automated decision making and profiling.

Data Security incidents

Any security incidents which may impact on the confidentiality, integrity or availability of personal data held by us must be reported immediately to the Data Protection Lead by {DESCRIBE PROCESS FOR REPORTING INCIDENTS}

Such events could include:

- Loss of records, laptops or media containing personal data;
- Unauthorised access to information systems containing personal data;
- Access of personal data with no justifiable business need;
- Personal data being misdirected to an incorrect recipient;
- Loss of access to systems containing personal data.

All reported incidents will be recorded to ensure appropriate mitigation measures are in place and to identify lessons or necessary improvements.

The Data Protection Lead will consider whether the incident meets the GDPR definition of a "personal data breach" which presents a risk to individuals. He/she will present a report to the Chief Executive {or SIRO where designated} including a recommendation on whether to report the matter to the Information Commissioner's Office.

If the Chief Executive {or SIRO where designated} decides that an incident constitutes a reportable data breach, the DP Lead will report the incident to the ICO and liaise as appropriate.

If a data breach presents a high risk to the data subjects, the DP Lead will ensure that they are also notified of the breach.

For further detail see the **Personal Data *Incident and Breach Reporting Procedure***.

See also: European Data Protection Board Guidelines on Personal Data Breach Reporting and relevant ICO Guidance.

Contact

Any questions about this policy should be directed to:

Data Protection Lead

{ NAME OF DATA PROTECTION CONTACT}

{ADDRESS}

{EMAIL}

{PHONE NUMBER}