# DATA PROTECTION POLICY

**Date Written:** August 2024
**Date Reviewed:** August 2025
**Date for next review:** August 2026
**Policy Owner:** Head of Communications & Impact

**Introduction**

This Policy sets out the obligations of the organisation, in respect of personal data under EU Regulation 2016/679 General Data Protection Regulation (GDPR).

The GDPR defines personal data:

*any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.*

This policy is a summary of the organisation's commitment to the legislation. Further information, where necessary, will be sought via the Information Commissioner's Office.

**The Data Protection Principles**

All personal data must be:

1.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

1.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

1.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

1.4 Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

1.5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR

in order to safeguard the rights and freedoms of the data subject.

1.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

**The Rights of Data Subjects**

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

1.7 The right to be informed (Part 12).

1.8 The right of access (Part 13);

1.9 The right to rectification (Part 14);

1.10 The right to erasure (also known as the 'right to be forgotten') (Part 15);

1.11 The right to restrict processing (Part 16);

1.12 The right to data portability (Part 17);

1.13 The right to object (Part 18); and

1.14 Rights with respect to automated decision-making and profiling (Parts 19 and 20).

The Data Protection Officer for the organisation is: Sophie Jerrold

**Key principles:**

- Data subjects will be asked to provide explicit consent for collection and processing
- The data will be accurate
- Will establish there is a need to collect the data
- If data falls within a 'special category' (also known as sensitive personal data eg data concerning race, ethnicity, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation), then additional conditions will be met.

1.15 data subjects are kept informed at all times of the purpose or purposes for which the organisation uses their personal data.

1.16 Will only collect and process data for as long as necessary

1.17 Will comply with requests from data subject to access data, and any subsequent requests (see section 4)

**Data Subject Access**

1.18 Data subjects may make subject access requests (SAR) at any time to find out more about the personal data which the Organisation holds about them, what it is doing with that personal data, and why.

1.19 Data subjects wishing to make a SAR should make the request in writing to the Organisation's Data Protection Officer.

1.20 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If

such additional time is required, the employee data subject shall be informed.

1.21 The Organisation does not charge a fee for the handling of normal SARs. The Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to an employee data subject, and for requests that excessive.

1.22 Data subjects have the right to require the Organisation to rectify any of their personal data that is inaccurate or incomplete. The organisation will inform the data subject of that rectification, within one month of the request.

1.23 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

1.24 Data subjects have the right to request that the Organisation erases the personal data it holds about them in the following circumstances:

1.24.1 It is no longer necessary for the Organisation to hold it

1.24.2 The employee wishes to withdraw their consent

1.24.3 The data subjects objects to the Organisation holding and processing their personal data

1.24.4 The personal data has been processed unlawfully;

1.24.5 The personal data needs to be erased in order for the Organisation to comply with a particular legal obligation, or the personal data is being held and processed for the purpose of providing information society services to a child.

1.25 Unless the Organisation has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request.

1.26 Data subjects may request that the Organisation ceases processing the personal data it holds about them. If an data subject makes such a request, the Organisation shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

1.27 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

1.28 Data subjects have the right to object to the Organisation processing their personal data based on legitimate interests, **[**direct marketing (including profiling),**]** **[**and processing for scientific and/or historical research and statistics purposes**]**.

1.29 Where an data subject objects to the Organisation processing their personal data based on its legitimate interests, the Organisation shall cease such processing immediately, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

1.30 Where an data subject objects to the Organisation processing their personal data for direct marketing purposes, the Organisation shall cease such processing immediately.

1.31 The Organisation holds personal data that is directly relevant to its employees. That personal data shall be collected, held, and processed in accordance with Data subjects' rights and the Organisation's

obligations under the GDPR and with this Policy.

1.32 Data subjects have the right to request that the Organisation does not keep health records about them.

**Data Security**

All data, both electronic and hard copy, will be managed with integrity including
Passwords used to protect the data, and not shared
No data stored on removable devices
All data to be disposed of securely
All information will not be shared informally
All stakeholders to be informed of management of data

**Data Breach Notification**

1.33 All personal data breaches must be reported immediately to the organisation's Data Protection Officer.

1.34 Current guidance from the ICO will be used to manage these issues.