BRATHAY TRUST

DATA PROTECTION POLICY

POLICY & MANAGEMENT GUIDELINES

DOCUMENT MANAGEMENT RECORD

DATA PROTECTION POLICY & MANAGEMENT GUIDELINES

Originated: July 2010
Next Full Document Review Date: May 2021

Document Status				
Issue	Date	Notes	Originator	Authorised for use by:
1	July 2010	Draft Document Issued for consultation	CEO office	Trustees
2.	August 2010	Document distributed to staff	CEO office	Leadership & Management Teams
3.	Sept 2011	Edited to include Security breach guidelines & link to ICT Security policy	CEO Office	Management Group
4.	May 2013	Updated in line with policy refresh dates	CEO Office	Leadership Team
5.	August 2015	Updated for changes in responsibilities	Finance Director	
6.	June 2016	Reviewed and format updated	Operations Manager Finance	Finance Director
7.	April 2018	Major rewrite due to legislation changes	Compliance Manager	Senior Management Team
8.	May 2018	Document distributed to staff on the intranet	Compliance Manager	

CONTENTS **PAGE**

INTRODUCTION

This Policy sets out the obligations of Brathay Trust (Brathay) regarding data protection and the rights of customers, business contacts, employees, workers, volunteers, participants, supporters, donors and any other data subjects in respect of their personal data under Data Protection Legislation such as EU Regulation 2016/679 General Data Protection Regulation (GDPR) and the Data Protection Act (DPA).

It also sets our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by Brathay, its employees, agents, contractors or any other parties working on behalf of Brathay.

Brathay is registered with the Information Commissioner's Office under registration reference Z6373431. As a Controller of personal data, Brathay recognises its duty to ensure that all such data is handled properly and confidentially at all times, irrespective of whether it is held on paper or by electronic means and covers the whole lifecycle of it.

DATA PROTECTION PRINCIPLES

Data Protection Legislation sets out the following six principles with which anyone handling personal data must comply:

1. Processing must be lawful, fair and transparent
2. The purposes of processing must be specified, explicit and legitimate
3. Personal data must be adequate, relevant and not excessive
4. Personal data must be accurate and kept up to date
5. Personal data must be kept for no longer than necessary
6. Personal data must be processed in a secure manner

Principle 1 Lawful, Fair, and Transparent Data Processing

Data Protection Legislation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Data Protection Legislation (Article 6 of the GDPR) states that processing of personal data shall be lawful if at least one of the lawful bases for processing applies:

- **Consent:** the individual has given clear consent for us to process their personal data for one or more specific purposes
- **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract with them
- **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations)
- **Vital interests:** the processing is necessary to protect someone's life
- **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law
- **Legitimate interests:** the processing is necessary for the purposes of our legitimate interests or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

If the information is "special category data" (sensitive personal data) and is data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric information, health and sex life or sexual orientation, we must ensure that at least one of following conditions is met (in addition to the lawful basis above):

- The data subject has given their explicit consent to the processing of such data for one or more specified purposes
- The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent

- The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects
- The processing relates to personal data which is clearly made public by the data subject
- The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity
- The processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject
- The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR
- The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy) or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

To process personal data about criminal convictions or offences, we must have both lawful basis and either legal authority or official authority for the processing. The rules for sensitive ('special category') do not apply to information about criminal allegations, proceeding or convictions. Instead, there are separate safeguards for this kind of personal data as set out in Article 10 of the GDPR. This means that Brathay must either be processing the data in an official capacity or have specific legal authorisation to do so.

Principle 2 Specified, Explicit, and Legitimate Purposes
Brathay collects and processes personal data which is collected directly from data subjects and obtained from third parties. Data subjects are kept informed of the purpose or purposes for which Brathay uses their personal data. Please refer to section 'Keeping Data Subjects Informed' for more information on keeping data subjects informed.

Principle 3 Adequate, Relevant and Limited Data Processing
Brathay will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed).

Principle 4 Accuracy of Data and Keeping Data Up-to-Date
Brathay shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in section 'Rectification of Personal Data' below.

The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

Principle 5 Data Retention
Brathay shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay. For details of Brathay's approach to data retention, including retention periods for specific legal and statutory data types, please refer to our Records Management Policy and Document Retention Schedule.

Principle 6 Secure Processing
Brathay shall ensure that all personal data collected, held and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

RIGHTS OF DATA SUBJECTS

Data Protection Legislation sets out the following rights applicable to data subjects:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure (also known as the 'right to be forgotten')
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights with respect to automated decision-making and profiling

The Right to Be Informed
Accountability and Record-Keeping
Brathay's Data Protection Officer is Heather Dixon, Finance Director and can be contacted by emailing data-protection@brathay.org.uk or by post c/o Brathay Trust, Brathay Hall, Ambleside, Cumbria, LA22 0HP.

The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Brathay's other Information Governance related policies, with Data Protection Legislation and other applicable data protection legislation.

Brathay keeps written internal records of all personal data collection, holding and processing, which incorporates the following information:

- The name and details of Brathay, its Data Protection Officer and any applicable third-party data processors
- The purposes for which Brathay collects, holds and processes personal data
- Details of the categories of personal data collected, held and processed by Brathay and the categories of data subject to which that personal data relates
- Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards
- Details of how long personal data will be retained by Brathay
- Detailed descriptions of all technical and organisational measures taken by Brathay to ensure the security of personal data.

Keeping Data Subjects Informed (Privacy Rights)

Brathay has an overarching and organisational Privacy Policy that underpins all departmental privacy notices. Privacy notices are the best way for us to tell individuals (e.g. clients, staff, delegates, parents, volunteers, etc) why and how we use personal and sensitive information (PSI). The notices are used to share the specific detail on personal data processes that we have in place across departments and teams.

Brathay will provide this information to every data subject:

- Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
    - if the personal data is used to communicate with the data subject, when the first communication is made; or
    - if the personal data is to be transferred to another party, before that transfer is made; or
    - as soon as reasonably possible after the personal data is obtained.

The following information will be provided, usually in departmental privacy notices:

- The purpose(s) for which the personal data is being collected and will be processed and the legal basis justifying that collection and processing
- Where applicable, the legitimate interests upon which Brathay is justifying its collection and processing of the personal data
- Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed
- Where the personal data is to be transferred to one or more third parties, details of those parties
- Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (EEA), details of that transfer, including but not limited to the safeguards in place
- Details of data retention
- Details of the data subject's rights under Data Protection Legislation
- Where applicable, details of the data subject's right to withdraw their consent to Brathay's processing of their personal data at any time
- Details of the data subject's right to complain to the Information Commissioner's Office, our regulator
- Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data
- Where applicable, details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions and any consequences.

The Right of Access (Subject Access Requests)

Data subjects may make Subject Access Requests (SAR) at any time to find out more about the personal data which Brathay holds about them, what it is doing with that personal data and why.
Anyone wishing to make a SAR must complete the Subject Access Request Form and send to Brathay's Data Protection Officer at email data-protection@brathay.org.uk or post c/o Brathay Trust, Brathay Hall, Ambleside, Cumbria, LA22 0HP.

Responses to SARs shall normally be made within 30 calendar days of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If

additional time is required, the data subject will be notified.

All SARs received shall be handled by the Data Protection Officer who will be supported by staff from other departments when requested.

We do not charge a fee for the handling of normal SARs but we reserve the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and/or for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

The Right to Rectification
Data subjects have the right to require us to rectify any of their personal data that is inaccurate or incomplete. We will rectify the personal data in question and inform the data subject of that rectification, within one month of the data subject informing Brathay of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

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.

The Right to Erasure ('the right to be forgotten')
Data subjects have the right to request that Brathay erases the personal data we hold about them in the following circumstances:

- It is no longer necessary for us to hold that personal data with respect to the purpose(s) for which it was originally collected or processed
- The data subject wishes to withdraw their consent to Brathay holding and processing their personal data
- The data subject objects to Brathay holding and processing their personal data (and there is no overriding legitimate interest to allow Brathay to continue doing so)
- The personal data has been processed unlawfully
- The personal data needs to be erased in order for Brathay to comply with a particular legal obligation
- The personal data is being held and processed for the purpose of providing information services to a child.

Unless Brathay 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 30 calendar days of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

The Right to Restrict Processing
Data subjects may request that we cease processing the personal data we holds about them. If a data subject makes such a request, Brathay will 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.

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).

The Right to Data Portability
Business processes should allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without any hindrance to the usability of the data.

The right to data portability only applies when each of the following are met:

- The personal data an individual has provided to a controller
- Where the processing is based on the individual's consent or the performance of a contract
- When processing is carried out by automated means.

'Processing by automated means' is defined as personal data processed electronically, for example on a computer, smart phone or call recording software.

The Right to Object
Data subjects have the right to object to Brathay processing their personal data based on legitimate interests, direct marketing (including profiling) and processing for scientific and/or historical research and statistics purposes.

Where a data subject objects to Brathay processing their personal data based on our legitimate interests, we will cease such processing immediately, unless it can be demonstrated that Brathay'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.

Where a data subject objects to Brathay processing their personal data for direct marketing purposes, Brathay shall cease such processing immediately.

Rights with Respect to Automated Decision Making and Profiling
<u>Automated Decision Making</u>
Brathay does not usually use personal data in any automated decision-making processes.

Where such decisions have a legal (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from Brathay.

The right described above does not apply in the following circumstances:

- The decision is necessary for the entry into, or performance of, a contract between Brathay and the data subject;
- The decision is authorised by law; or
- The data subject has given their explicit consent.

<u>Profiling</u>
Brathay may use personal data for profiling purposes.

When personal data is used for profiling purposes, the following shall apply:

- Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling
- Appropriate mathematical or statistical procedures shall be used

- Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
- All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

DATA SECURITY

Transferring Personal Data and Communications

Brathay will ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- Personal data must never be included within the subject line or message body of an email
- All personal data legitimately transmitted via IT systems (e.g. email) must be protected by the use of a strong password and marked "confidential"
- Personal data may be transmitted over secure networks only. Transmission over unsecured networks is not permitted in any circumstances
- Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable
- Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated must also be deleted
- Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data
- Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery post and
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic encrypted media shall be transferred in a suitable container marked "confidential".

Storage

Brathay shall ensure that the following measures are taken with respect to the storage of personal data:

- All electronic copies of personal data should be stored securely either by using passwords or restricted permissions on folders
- All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar
- All personal data stored electronically should be backed up daily with backups stored offsite. All backups are encrypted
- No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to Brathay or otherwise without the formal written approval of the appropriate member of the Senior Management Team and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary
- No personal data should be transferred to any personal device belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of Brathay where the party in question has agreed to comply fully with this Policy and of Data Protection Legislation (which may include demonstrating to Brathay that all suitable technical and organisational measures have been taken).

Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

Use of Personal Data

Brathay shall ensure that the following measures are taken with respect to the use of personal data:

- Personal data processed by Brathay must only be used for the purpose it was collected for
- No personal data may be shared informally and/or transferred to an employee, agent, sub-contractor, or other party working on behalf of Brathay. If they require access to any personal data that they do not already have access to, such access should be formally requested from the relevant member of the Senior Management Team.
- Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time
- Where personal data held by Brathay is used for marketing purposes, it shall be the responsibility of the nominated person in each department to ensure that the appropriate consent is obtained, documented for as long as deemed necessary and that no data subjects have opted out, whether directly or via a third-party service (e.g. the Telephone Preference Service).

IT Security

Brathay shall ensure that the following measures are taken with respect to IT and information security:

- All passwords used to protect personal data are to be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. All software used by Brathay is designed to require such passwords.
- Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of Brathay, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords
- All software (including, but not limited to, applications and operating systems) will be kept up-to-date. Brathay's IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible
- No software may be installed on any Brathay-owned computer or device without the prior approval of the ICT Officer.

Organisational Measures

Brathay shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- All employees, agents, contractors, or other parties working on behalf of Brathay shall be made fully aware of both their individual responsibilities and Brathay's responsibilities under Data Protection Legislation and under this Policy and shall be provided with a copy of this Policy
- Only employees, agents, sub-contractors, or other parties working on behalf of Brathay that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by Brathay
- All employees, agents, contractors, or other parties working on behalf of Brathay handling personal data will be appropriately trained to do so
- All employees, agents, contractors, or other parties working on behalf of Brathay handling personal data will be appropriately supervised
- All employees, agents, contractors, or other parties working on behalf of Brathay handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise

- Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed
- All personal data held by Brathay shall be reviewed regularly
- The performance of those employees, agents, contractors or other parties working on behalf of Brathay handling personal data shall be regularly evaluated and reviewed
- All employees, agents, contractors, or other parties working on behalf of Brathay handling personal data will be bound to do so in accordance with the principles of Data Protection Legislation and this Policy by contract
- All agents, contractors, or other parties working on behalf of Brathay handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of Brathay arising out of this Policy and Data Protection Legislation
- Where any agent, contractor or other party working on behalf of Brathay handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless Brathay against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Transferring Personal Data to a Country Outside the EEA

Brathay may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

- The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data
- The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority
- The transfer is made with the informed consent of the relevant data subject(s)
- The transfer is necessary for the performance of a contract between the data subject and Brathay (or for pre-contractual steps taken at the request of the data subject)
- The transfer is necessary for important public interest reasons
- The transfer is necessary for the conduct of legal claims
- The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent
- The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

Data Breach Notification

Data should be protected at all times, this includes practical approaches such as locking away laptops when not in use and being careful who has access to where data is stored.

Any loss of personal data is a security breach and all breaches, near-misses and incidents must be

reported using the Data Protection Incident Report Form immediately to Brathay's Data Protection Officer by email to data-protection@brathay.org.uk

If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Officer will ensure that all affected data subjects are informed of the breach directly and without undue delay.

Data breach notifications will include the following information:

- The categories and approximate number of data subjects concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of Brathay's Data Protection Officer
- The likely consequences of the breach
- Details of the measures taken, or proposed to be taken, by Brathay to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

TRAINING

It is the aim of Brathay that all Workers will be fully informed of their obligations under the DPA and aware of their personal responsibilities. A tutorial is included in new starter inductions and managers provide department specific training. Periodic refresher sessions are also made available.

RESPONSIBILITIES

Trustees

Responsible for:

- Overall responsibility for a policy which ensures compliance with the relevant statutes

Chief Executive & Executive Team

Responsible for:

- Development and maintenance of such procedures as are necessary to ensure implementation of the policy
- Maintenance of the policy

Management

Responsible for:

- Design of procedures
- Implementation of procedures
- Dissemination throughout their team
- Ensuring day to day operational compliance
- Reporting to the Executive Team

Individual Responsibility (Workers and Contractors)

Responsible for:

- Compliance with procedures
- Identifying potential improvements through day to day work
- Reporting to the Management Team
- Reporting data incidents and near misses to the Data Protection Officer

APPENDIX 1 - Other relevant documents or policies

This policy should be used in conjunction with these Brathay documents:

- Data Protection Incident Form
- Information Sharing Policy and Agreement template
- Information Security Policy
- Records Management Policy
- Document Retention Schedule
- Privacy Policy
- Privacy Notice Code of Practice & Checklist
- Direct Marketing Code of Practice & Checklist
- ICT Policy
- ICT Handbook
- Disciplinary Policy
- Subject Access Request form
- Surveillance CCTV Code of Practice, Checklist and Privacy Impact Assessment
- Info Gov Risk Assessments

APPENDIX 2 - Key definitions

Personal Data - Any information relating to an identified or identifiable living individual.

Identifiable living individual – A living individual who can be identified, directly or indirectly, in particular by reference to:

- An identifier such as a name, identification number, location data or an online identifier; or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

Processing - an operation or set of operations which is performed on personal data or on sets of personal data such as:

- Collection, recording, organisation, structuring or storage
- Adaption or alternation
- Retrieval, consultation or use
- Disclosure by transmission, dissemination or otherwise making available
- Alignment or combination
- Restriction, erasure or destruction

Data Subject – The identified or identifiable living individual to whom personal data relates

Controller – The natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data

Processor – The natural or legal person which processes personal data on behalf of the controller

Special Category Data – also known as 'sensitive personal data' and includes:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health
- Sexual life and sexual orientation
- Genetic and biometric information

Information Commissioner's Office – The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

Source of key definitions: https://ico.org.uk/