BRATHAY TRUST

DATA PROTECTION POLICY

POLICY & MANAGEMENT GUIDELINES

DOCUMENT MANAGEMENT RECORD

Policy Name: Data Protection
Date: September 2023
Review Date: September 2026
Policy Owner: Compliance Manager
Distribution: Internal and External – Non- Confidential, website

SUMMARY POLICY STATEMENT

This Data Protection Policy is the overarching policy for data security and protection for Brathay Trust including Brathay Services Limited.

The purpose of the Data Protection Policy is to support the work we do and to adhere to the General Data Protection Regulation, the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy covers

- Our data protection principles and commitment to common law and legislative compliance
- Procedures for data protection by design and by default
- All data which we process either in hardcopy or digital copy, this includes special categories of data.

This policy applies to all staff, including temporary staff, workers, volunteers, contractors and any other relevant third parties.

PRINCIPLES

We establish and maintain policies to ensure compliance with the Data Protection Act 2018, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

We establish and maintain procedures for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and consent.

Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them. We ensure that it is as easy to withdraw as to give consent.

We undertake annual audits and spot checks of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’)
- Accurate and kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’)
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the GDPR, the right to:

- be informed
- access
- rectification
- erasure
- restrict processing
- data portability
- object
- Rights in relation to automated decision making and profiling.

Although we are not legally obliged to appoint a Data Protection Officer (DPO) we have done so to demonstrate our commitment to data protection best practice. The DPO will report to the highest management level of the organisation.

Brathay's Data Protection Officer is Heather Jones, Compliance Manager and can be contacted by emailing data-protection@brathay.org.uk or by post c/o Brathay Trust, Brathay Hall, Ambleside, Cumbria, LA22 0HP.

Brathay supports the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise and ongoing training. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

We complete the NHS Data Security and Protection Toolkit on an annual basis and our publication status can be found here: Organisation Details (dsptoolkit.nhs.uk)

PRIVACY BY DESIGN & DEFAULT

We implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.
Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

All new systems used for data processing will have data protection built in from the beginning of the system change.

All existing data processing has been recorded on our departmental Information Asset Register.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we use pseudonymised data to protect the privacy and confidentiality of our staff and those we support and work with.

TRAINING

It is the aim of Brathay that all employees, workers, agents, volunteers, contractors and/or other relevant parties will be fully informed of their obligations under Data Protection Legislation as well as of their personal responsibilities. A mandatory online training is provided when joining as well as annual refreshers given. Managers provide tailored training and guidance in departmental processes and procedures.

RESPONSIBILITIES

Trustees

Responsible for:

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

Chief Executive & Leadership Team

Responsible for:

- Development and maintenance of such procedures as are necessary to ensure implementation of the policy
- Maintenance of the policy
- Reporting data security breaches, incidents and near misses to the Data Protection Officer

Management

Responsible for:

- Design of procedures
- Implementation of procedures
- Dissemination throughout their team
- Ensuring staff receive the relevant induction and refresher training
- Ensuring that the design of departmental procedures allows for day-to-day operational compliance
- Ensuring that the implementation of procedures is in line with policy
- Reporting to the Leadership Team
- Communicating policy and encouraging discussion throughout their team via team meetings, 121s etc.
- Familiarising staff with when and how to use the Data & Security Protection Report Form
- Reporting data security breaches, incidents and near misses to the Data Protection Officer

Individual Responsibility (Employees, Workers, Agents Contractors and Other Parties)

Responsible for:

- Compliance with policy and procedures
- Complete mandatory training and subsequent refreshers
- Recognise a Subject Access Request (SAR) and know what to do
- Know how to report data security breaches, incidents and near misses
- Reporting data security breaches, incidents and near misses to the Data Protection Officer
- Identifying potential improvements through day-to-day work
- Reporting to the Management Team
- Know how to share personal data securely
- Know what to do when you are away from the office

The Data Protection Officer (DPO)

The key responsibilities of the DPO are:

- Consulting on changes to systems and processes
- Monitoring compliance with the GDPR and the Data Protection Act 2018
- Reviewing and signing off DPIA
- Reporting on data protection and compliance with legislation to senior management
- Liaising, if required, with the Information Commissioner's Office (ICO)

ASSOCIATED GUIDANCE AND DOCUMENTS

This policy is underpinned by the following:

- Departmental data processing procedures
- Records management policy
- IT and digital policy
- Data breach procedures, including the data security & protection report form
- Subject access request form and procedures
- Document retention schedule
- Data quality and record keeping guidance
- Business continuity plan
- Privacy policy and departmental privacy notices
- Privacy notice code of practice and checklist
- Data classification and handling procedures
- Whistleblowing policy
- Data processor agreement template
- Information sharing policy and agreement template
- Surveillance CCTV code of practice and checklist
- Information governance risk assessment
- Information asset registers
- Disciplinary policy
- Relevant sections on the staff intranet.