BRATHAY TRUST

DATA PROTECTION POLICY

POLICY & MANAGEMENT GUIDELINES

DOCUMENT MANAGEMENT RECORD

Policy Name: Data Protection
Date: June 2021
Review Date: June 2024
Policy Owner: Compliance Manager
Distribution: Internal and External – Non- Confidential, website

SUMMARY POLICY STATEMENT

This Policy sets out the obligations and commitments of Brathay Trust including Brathay Services Ltd (Brathay) regarding data protection and the rights of customers, business contacts, employees, workers, volunteers, participants, supporters, donors, members and any other data subjects in respect of their personal data under Data Protection Legislation such as the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR), the EU General Data Protection Regulation (EU GDPR).

It also sets our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must always be followed by Brathay, its employees, workers, 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 always handled properly and confidentially, irrespective of whether it is held on paper or by electronic means and covers the whole lifecycle of it.

Data protection is the responsibility of all employees, workers, agents, contractors and any other parties working on behalf of Brathay. All will comply with this Policy and, where applicable, must implement such practices, processes, controls and training as are reasonably necessary to ensure such compliance.
At times our clients may ask us to follow certain frameworks, protocols or other ways of working, this Policy compliments those and must be used in conjunction with the client's requirements. For example, our work with the NHS also sets out our compliance commitment with the 10 Data Security Standards, the Caldicott Principles and the Data Security & Protection Toolkit, including an annual self-assessment. All staff working on these types of contract will know and understand their responsibilities, expectations and requirements.

DATA PROTECTION PRINCIPLES

This Policy aims to ensure compliance with Data Protection Legislation (including the DPA, UK and EU GDPR). As a Data Controller, Brathay are responsible for, and must demonstrate, such compliance. Data Protection Legislation sets out the following seven 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
7. Be responsible for personal data and be able to demonstrate compliance (accountability)

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 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, it must be freely given and can be withdrawn at any time by data subjects
- **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" (also referred to as 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 the UK and EU 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 UK and EU GDPR based on UK, EU or EU Member State law (if applicable) 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 the UK and EU 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 (Purpose limitation)
Brathay collects and processes personal data which is collected directly from data subjects and obtained from third parties. The data collected is only used for the reason it was collected. 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.

Principle 3
Adequate, Relevant and Limited Data Processing (Data minimisation)
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).

Employees, workers, agents, contractors or other parties working on behalf of Brathay may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.

Employees, workers, agents, contractors or other parties working on behalf of Brathay may process personal data only when the performance of their job duties requires it. Personal data held by Brathay cannot be processed for any unrelated reasons.

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 will 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.

Brathay staff ensures the accuracy in our data in both hardcopy and digital records by making sure all data has the following characteristics:

- Authentic – e.g. the data is what is claims to be, has been created or sent by the person who said that they created or sent it, and that this was done at the time claimed
- Reliable – e.g. the data is complete, accurate, has been created close to the time of the activity it records, and has been created by individuals with direct knowledge of the event it records
- Integrity – e.g. the data is complete and unaltered, it is also protected from being changed or altered by unauthorised persons, any alterations are clearly marked and the person who made them can be identified
- Useable – e.g. the data can be located when it is required for use and its context is clear in a contemporaneous record.

Principle 5
Data Retention (Storage Limitation)
Brathay staff shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that 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 securely and 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
Integrity and confidentiality (Security)
Brathay staff 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. Data must be protected at all times, this includes practical approaches such as maintaining a clear desk policy, locking away laptops when not in use, using locked boxes to transport documents outside the building, shredding documents when no longer needed and being careful who has access to where data is stored.

All technical, physical and other organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data. Spot checks and audits will be led by the Data Protection Officer at least annually. The findings will be recorded and reported to the relevant managers and the Leadership Team.

Data security must be maintained at all times by protecting the confidentiality, integrity and availability of all personal data as follows:

- Only those with a genuine need to access and use personal data and who are authorised to do so may access and use it

- Only those with a genuine need to access and use personal data and who are authorised to do so may access and use it
- Personal data must be accurate and suitable for the purpose of purposes for which it is collected, held and processed
- Authorised users must always be able to access the personal data as required for the authorised purpose or purposes
- IT will centrally manage device policies to ensure the appropriate levels of technical measures are in place.

Principle 7
Accountability

Brathay shall be responsible for complying with Data Protection Legislation and that it will demonstrate this compliance by having appropriate technical and organisational measures in place to meet the requirements of accountability. This will include adopting and implementing policies and procedures, taking a 'data protection by design' approach, having written contracts in place with third parties, maintaining records of processing activities, having a breach management system and implementing appropriate security measures. Being accountable for data protection can help Brathay build trust with individuals and may also help mitigate any regulator enforcement action.

Data security and protection is the responsibility of all employees, workers, agents, contractors and any other parties working on behalf of Brathay. All must comply with Data Protection Legislation, this Policy and, where applicable, must implement such practices, processes, controls and training as are reasonably necessary to ensure such compliance. Appropriate training is provided in data protection, cyber security and privacy, department procedures, the relevant aspects of Data Protection Legislation, this Policy and any other applicable policies.

Managers will ensure that their departments keep an up-to-date written records in the form of Information Asset Registers (IAR) and departmental privacy notices that document all personal data processing in their area. These departmental Information Asset Registers form Brathay's overarching Register of Processing Activities (ROPA) as required by the Data Protection Legislation.

The departmental Information Asset Registers will include:

- The purposes for which Brathay collects, holds and processes personal data
- Details of who this information is shared with including joint controllers and data processors
- 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 countries including all mechanisms and security safeguards
- The lawful basis for processing, including conditions for processing special categories and criminal offence data
- Details of how long personal data will be kept by Brathay
- Detailed descriptions of all technical and organisational measures taken to ensure the security of personal data.
- Information Asset Registers will be assigned Information Asset Owners who are responsible for ensuring their department's register is kept up to date.

Another aspect of being accountable is ensuring that agreements and contracts are in place before Brathay shares personal data with partners, processors and other third parties. There are different agreements depending on the relationships and each sets out the responsibilities of the parties:

- **Information Sharing Agreement** are used when sharing data with partners and other organisations. Examples include auditors or partners in the care sector. Staff should refer to

the Information Sharing Policy and the template Information Sharing Agreement on the intranet for further details.

- **Data Processor Agreements** are required every time third parties are employed to process personal data under Brathay's instruction as a Controller. Examples include external organisations that process payroll, provide IT support services, etc. Both parties, the Controller (Brathay) and Processor have responsibilities for non-compliance with legislation. Some Processors will have clauses built into the contract that cover the details of data processing and responsibilities, but if not, then a Data Processor agreement must be developed. A template Processor Agreement is available on the intranet.

In both instances, a signed and current copy of the agreement must be kept on file by the responsible manager.

The Data Protection Officer is responsible for administering this Policy and for developing and implementing any applicable related policies and organisational guidance. Brathay's data protection compliance will be regularly reviewed and evaluated by means of data protection audits and spot checks. Accountability obligations are ongoing and it is therefore important to continue to review, evaluate and update measures.

RIGHTS OF DATA SUBJECTS

We uphold the personal data rights as outline in the UK and EU GDPR

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
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 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.

The Data Protection Officer is responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, Brathay's other Information Governance related policies and with Data Protection Legislation. Brathay aims to establish best practice and ensure learning is shared effectively.

The Data Protection Officer is responsible for delivering an agreed annual programme of audits and spot checks. The findings and recommendations are documented shared with the appropriate managers for action and mitigation of risk. The results reported to the Leadership Team.

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

- The name and details of Brathay and its Data Protection Officer
- Details of applicable third-party data processors and copies of the contracts
- Details of Processor / Information Sharing Agreements with partners and third parties
- Departmental privacy notices

- A Document Retention Schedule
- Information Governance risk assessments
- Departments will have up to date Information Asset Registers (IAR)

Keeping Data Subjects Informed (Privacy Rights)

Brathay has an overarching organisational Privacy Policy that underpins all departmental privacy notices. Departmental 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. 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 lawful basis justifying that collection and processing
- Where applicable, the legitimate interests upon which Brathay is justifying its collection and processing of the data
- Where the 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, th details of those parties
- Where the personal data is to be transferred to a third party that is located outside of the UK details of that transfer, including but not limited to the safeguards in place
- Details of how long it is kept
- 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
- Reference or a link to Brathay's overarching organisational Privacy Policy.

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. They may also wish to correct or change the data we hold.

All staff are responsible for knowing how to recognise a SAR and that the request must be managed through the SAR process. Staff should provide data subjects with a copy of the SAR form which details what happens next and how to make the SAR.

Anyone wishing to make a request should 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 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 additional time is required, the data subject will be notified.

All SARs received are 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 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

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 1 month 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 hold 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 UK and EU 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.

Profiling

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.

RISK ASSESSMENTS AND PRIVACY BY DESIGN

In accordance with privacy by design principles, Brathay will carry out Information Governance Risk Assessments for any and all new projects and/or new uses of personal data that involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects. This is to ensure that new systems and changes in process will have data protection built in from the beginning, this is known as privacy by design.

The principles of privacy by design are to be followed at all times when collecting, holding and processing personal data. The following factors will be taken into consideration when completing the Information Governance Risk Assessments:

- The nature, scope, context and purpose or purposes of the collection, handling and processing
- The state of the art of all relevant technical and organisational measures to be taken
- The cost of implementing such measures
- The risk posed to data subjects and to Brathay, including their likelihood and severity.

All completed Information Governance Risk Assessments must be forwarded to data-protection@brathay.org.uk for review and sign off.

DIRECT MARKETING

Brathay is subject to certain rules and regulations when marketing our products and services, all staff who send direct marketing are to adhere to the Direct Marketing Code of Practice and Checklist.

In many cases the prior consent of data subjects is required for electronic directly marketing (e.g. email, text messaging), subject to the following exception:

- Brathay may send marketing text messages and emails to a customer provided that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from us.

The right to object to direct marketing will be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve clarity. If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.

DATA SECURITY

Data security is focussed on guaranteeing availability (ensuring that authorised users always have access to information when they need it), integrity (safeguarding its accuracy and completeness) and confidentiality (ensuring that sensitive information is accessible only to those authorised to use it).

Brathay will implement appropriate organisational, physical and technical measures to uphold the data protection principles mentioned above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights.

All employees, workers, agents and contractors will follow all of the requirements and expectations as set out in this policy as well as the IT & Digital Systems policy and accompanying procedures.

Transferring Personal Data and Communications

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

- Personal data should not 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 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 transferred in hardcopy form it should be passed directly to the recipient or sent using Special Delivery post
- All personal data to be transferred physically, whether in hardcopy form or on removable electronic encrypted media shall be transferred in a suitable and secure container (e.g. a locked box).

Storage

Brathay staff 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 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. Keys to lockable storage must be held securely
- All hardcopies being transported outside of Brathay premises must be secured in locked boxes or other approved secure storage systems
- Automatic backups are done every working day
- Backups are encrypted and stored securely
- 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 Leadership 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 (e.g. using a shredder or placing in confidential shredding bags for hardcopies). When a third party is used to securely dispose of equipment or bags of confidential documents, a certificate of destruction must be requested from the third and obtained by the relevant department (e.g. IT, Estates, etc)

Use of Personal Data

Brathay staff will 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).

Organisational Measures

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

- All employees, workers, agents, contractors, or other parties working on behalf of Brathay will 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
    - handling personal data will be appropriately trained to do so
    - handling personal data will be appropriately supervised
    - 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
    - handling personal data will be bound to do so in accordance with the principles of Data Protection Legislation and this Policy by contract
- Only employees, workers, agents, 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
- 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, workers, agents, contractors or other parties working on behalf of Brathay handling personal data shall be regularly evaluated and reviewed
- All workers, 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 worker, 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 UK

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

The transfer of personal data to a country outside of the UK 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 UK and/or 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 UK and EU 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 Security and Breach Notification

All personal data breaches, or suspected breaches, must be reported without delay to Brathay's Data Protection Officer. It is better to report a breach even when not sure that it is one, as reporting near misses are just as important to report as actual breaches. This is how we learn and can hopefully prevent things happening in the future by sharing the learning and reviewing what happened to mitigate future risk. All breaches, suspected breaches, near-misses and incidents must be reported using the Data Security & Protection Incident Report Form available on the staff intranet.

As soon as an employee, worker, agent, contractor or other party working on Brathay's behalf becomes aware of or suspects that a personal data breach has occurred, they must report it immediately using the Data Security & Protection incident form and not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question must be carefully obtained, kept confidential and provided to the Data Protection Officer.

Where Brathay is a Processor of data and instructed by another organisation (known as the Controller), management and staff will ensure all terms of the contract are met and know how and when to report any data security and protection near misses, breaches or suspected breaches. The processes as set out by the Controller must be followed as well as reported through the Brathay incident reporting system as mentioned above.

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 harm or economic damage), the Data Protection Officer will 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.

For all breaches and near misses it is necessary for the Data Protection Officer to oversee or carry out a fact-finding investigation to establish (as a minimum):

- Why and how did it happen
- How could it have been prevented
- What is the impact
- How can we improve and reduce the risk of reoccurrence

These investigations may include relevant managers and other staff that have been involved in or need to be aware of the breach. If the breach is of a very serious nature and due to negligence of a staff member, sanctions may apply and/or the disciplinary process implemented.

If 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 security and 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 employees, workers, agents, contractors or other parties will be fully informed of their obligations under Data Protection Legislation as well as aware of their personal responsibilities. A mandatory training module is provided when joining as well as annual refreshers. Managers provide tailored training and guidance to departmental 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

DEFINITIONS / ABBREVIATIONS

Consent – The consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signify their agreement to the processing of personal data relating to them.

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

Data Subject –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
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

Information Commissioner's Office (ICO)– 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

Personal data – Any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, ID number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.

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.

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

Processor / Data Processor – The natural or legal person which processes personal data on behalf of the Controller

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

Special Category Data – Also referred to as 'sensitive personal data' and includes:

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

ASSOCIATED GUIDANCE AND DOCUMENTS

This policy should be used in conjunction other Brathay documents including but not limited to:

- Data Security & Protection Incident and Near Miss Report Form
- Information Governance Risk Assessment template
- Information Asset Register (by department)
- Information Sharing Policy & Agreement template
- Processor Agreement template
- Records Management Policy
- Document Retention Schedule
- Data Classifications and Handling Procedures
- Privacy Policy
- Privacy Notice Code of Practice & Checklist
- Direct Marketing Code of Practice & Checklist
- IT & Digital Systems Policy
- Disciplinary Policy
- Whistleblowing Policy
- Staff Handbook
- Subject Access Request form
- Surveillance CCTV Code of Practice, Checklist and Privacy Impact Assessment

Additional guidance and resources are available from these external websites:
Information Commissioner's office
https://ico.org.uk/

The Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

The UK General Data Protection Regulation
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

EU Regulation 2016/679 General Data Protection Regulation
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679

DOCUMENT HISTORY

Issue	Date	Notes	Author	Status
1.	August 2019	One-year review after GDPR implementation. Approved by Leadership Team	Compliance Manager	Approved
2.	May 2021	Review and updated based on changes in regulations. Approved by Leadership Team.	Compliance Manager	Approved
3.	June 2021	Approved electronically by Trustees and published on intranet and website	Compliance Manager	Approved
4.	July 2021	Formal Trustee approval	Compliance Manager	Approved