Number	Title	Owner	Last Updated	Next Review Date
2.4	Data and Privacy Protection	CEO	June2020	n/a

Policy Statement

British Exploring Society is committed to safeguarding the privacy of its stakeholders. We regard the lawful and correct treatment of personal information as critical to the successful delivery of our strategy, and to maintain the confidence between British Exploring Society and those with whom we deal.

To this extent, the Data and Privacy Protection Policy governs how (sensitive) personal information is collected, used, recorded, disclosed and stored, and what safeguards are in place.

British Exploring Society aims to adhere fully to the provisions of the Data Protection Act 1998 and the General Data Protection Regulations 2016. Failure to adhere to this Act is unlawful and could result in legal action against British Exploring Society, its staff, its volunteers or Trustees. A breach of any provision of the Act by either paid or unpaid staff will be regarded as extremely serious and will result in disciplinary action.

Further Policy Detail

Definitions

Data Owner – the person or entity which can authorise or deny access to certain data and is responsible for its accuracy and integrity.

Data Subject – the person or entity who is the subject of personal and sensitive information. Deceased persons or persons who cannot be distinguished from others are not considered Data Subjects under the Data Protection Act.

Data Controller – the person who determines the purpose for which, and the manner by which any personal data are processed. Under the Act, British Exploring Society is considered a Data Controller.

Data Processing – the carrying out of operations on data such as retrieving, transforming or classifying.

Provisions of the Data Protection Act

The Data Protection Act 1998 regulates the processing of personal and sensitive personal data of living and identifiable individuals. This includes the obtaining, holding, using or disclosing of such information and covers computerised records as well as manually filed records.

British Exploring Society's staff, volunteers and Trustees who process, use or have access to any personal information should ensure that the provisions of the Act are complied with at all times. These provisions can be summarized as follows:

- Data will be collected and processed fairly and lawfully;
- Data will only be collected and used for specified purposes;
- Data will be adequate, relevant and not excessive;
- Data will be accurate and up to date;
- Data will not be held any longer than necessary;
- Data will not be disclosed unlawfully;
- Data subject's rights will be respected;
- Data will be kept safe from unauthorised access, accidental loss or damage;
- Data will not routinely be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data[1].

Personal information and sensitive personal information

Personal information identifies someone as an individual, such as:

- Personal details;
- Family details;
- Lifestyle and social circumstances;
- Financial details;
- Education and employment;
- Images.

[1] In cases where British Exploring Society needs to provide personal data to local agents outside the European Economic Area (e.g. in order to apply for permits or to provide emergency support), it will endeavour to contract with such agents appropriately to protect the personal data of its stakeholders.

Sensitive personal information includes:

- Physical or mental health details;
- Racial or ethnic origin;
- Religious or other beliefs;
- Offences and alleged offences;
- Criminal proceedings, outcomes and sentences.

Data and Privacy Protection Procedures

Data collected, stored and used by British Exploring Society falls into two broad categories:

a. Internal data records: pertaining to staff, volunteers and trustees
b. External data records: pertaining to members, customers and clients.

The procedures below ensure that British Exploring Society meets its Data Protection responsibilities.

1. **Procedures for Internal Data Records**

Purpose
British Exploring Society obtains personal data (names, addresses, phone numbers, Next of Kin details, email addresses) via a number of sources including application forms and references. This data is stored and processed for the following purposes:

- Recruitment;
- Equal Opportunities monitoring;
- Volunteering opportunities;
- To distribute organisational material;
- Payroll;
- Access;
- To meet statutory obligations (Charity Commission, Companies House, etc.);
- To meet Health and Safety requirements.

Personal data of staff, volunteers and Trustees is only made available as appropriate to other staff and Trustees and will not be passed on to anyone outside the organisation without their explicit consent. Information supplied on application will be kept in soft copy and used only for the purpose for which it was supplied.

Staff and volunteer emergency contact details are kept securely for use in emergency situations.

Disclosures and Barring Services
British Exploring Society acts in accordance with the DBS's code of practice and takes all appropriate steps to secure enhanced DBS checks for trustees, staff and volunteers. Hard copies of disclosures are not routinely kept. In the majority of cases, hard copies are supplied and soft data is held by the umbrella body which processes British Exploring Society's DBS checks. British Exploring Society undertakes to ensure that no reproductions of any DBS certificate or its content are made without the explicit consent of DBS. We only share DBS certificate information with relevant persons in the course of their specific duties relevant to recruitment and vetting processes.

Accuracy and Access
Staff, volunteers and Trustees should be supplied with a copy of their personal data held by British Exploring Society if they request it from the CEO. Confidential mail for a staff member, volunteer or Trustee will be kept/forwarded to be opened by the addressee only. British Exploring Society operates a password-protected

computer system. Where personal and sensitive data relates to staff members, files are accessible only to appropriate members of staff. In the majority of cases, this will be limited to the CEO, Executive Assistant and members of the team responsible for safeguarding processes.

2. External Data Records

Purpose

British Exploring Society obtains personal data (e.g. names, addresses, phone numbers) and sensitive data such as medical information from members/clients and their Next of Kin. This data is obtained, stored and processed to assist staff and volunteers in the efficient running of services and to ensure high standards of care and positive experiences for explorers and leaders. This personal and sensitive data is stored and processed only for the purposes outlined in the agreement and service specification signed by clients or as otherwise authorised (for example by acknowledging terms and conditions online) by the client/member.

Consent

When an application to participate in an expedition is made, the terms and conditions of that application explain how data will be used, and applicants are required to acknowledge these terms and conditions. Personal and sensitive data may also be updated/collected by other means, e.g. phone or e-mail. This will only occur *after* clients/volunteers have consented to the collection of personal and sensitive data and will remain within the same scope of collection, processing and use as already consented to.

Our client groups

British Exploring Society is particularly mindful of the need to be sensitive to the needs of young and/or vulnerable data owners/subjects. Applicants under the age of 18 are required to secure adult consent for their participation in a British Exploring Society Expedition. British Exploring Society emphasises clear language and transparency in its written and verbal communication with clients under the age of 18 to ensure that they understand what we mean by sensitive and personal data. We explain to young clients what we intend to do with any data we collect, and explain their rights as a data subject/owner before they consent to give us any information. Personal data will not be passed on to anyone outside the organisation without explicit consent from the data owner unless there is a legal duty of disclosure.

Access

Only nominated British Exploring Society staff and volunteers are given access to personal and sensitive data. All staff, volunteers and trustees are made aware of our Data Protection Policy and of their obligation under this policy. Information supplied is kept in secure filing, paper and electronic systems and is only accessed by those individuals involved in the delivery of the service. Information will not be passed on to anyone outside the organisation without explicit consent. Some forms of such consent are included in our contractual arrangements with our clients in case of emergencies. Individuals will be supplied with a copy of any of their personal and sensitive data held by British Exploring Society as soon as possible and within a maximum of 30 days from when the request is made.

Accuracy

British Exploring Society takes regular steps to keep personal data up to date and accurate by contacting data subjects/owners. Personal and sensitive data will be stored/destroyed/de-identified according to the schedule and guidelines in Annex A. If we receive a request from an individual to amend their personal and sensitive records during our retention period, we will do so if we can verify the identity of the individual and can confirm the accuracy of the amend.

Sharing of data/Chain of Custody

Our activities require us from time to time to share specific personal and sensitive information with key staff and volunteers. Wherever possible this information remains digital, is password protected, and is retained within the CRM. Whilst on expedition, we may need to provide paper documentation to a limited number of individuals without digital access. In this case we will implement a Chain of Custody in order to assure the

location, status and subsequent safe destruction of any personal and sensitive data remote from British Exploring Society premises.

Storage
Personal data may be kept in paper-based systems and/or on a password-protected computer systems. Paper-based data are stored in organised systems. British Exploring Society enforces a clear desk and clear screen policy at all times.

Data and Privacy Protection Responsibilities

British Exploring Society, staff, volunteers and trustees may deal with personal and sensitive information from members/clients/volunteers.

Staff and volunteers are expected to operate a clear-desk policy and to be conscious at all times of the sensitivity of any information on-screen, on a printer, or in any other format. They may also be told or overhear sensitive information while working for/on behalf of British Exploring Society. Staff, paid or unpaid, must abide by this policy. The Council of Trustees is ultimately responsible for the implementation of this policy. British Exploring Society will ensure that all staff, volunteers and trustees receive adequate guidance in:

- The Data Protection Act as it affects the Charity;
- Our Data Protection Policy;
- Our systems;
- The individual obligations of staff, volunteers and trustees.

If any member of staff, volunteer or Trustee should have a concern on Data protection, he/she should immediately raise this in accordance with the Whistle-Blowing Policy.

Records Keeping

When beginning work with a new organisation, agent, referral partner or donor, British Exploring Society may elect to perform a process of due diligence to ensure the organisation is suitable. Any records kept as part of the Due Diligence process may have to be disclosed should the subject of that process request so. The Due Diligence process should follow the provisions of the British Exploring Society's Data Privacy and Protection Policy.

How is personal and sensitive personal information collected

Personal information and/or sensitive personal information may be collected in a variety of ways:

- Explorer and Volunteer applications;
- Competition entries;
- Expedition content – for example journals/diaries/projects;
- Additional recruitment data such as interviews and assessment notes;
- Fundraising events registrations;
- Donation pledges;
- Fundraising forms;
- Newsletter registrations;
- Requests for information;
- Volunteer feedback forms;
- Job applications;
- New staff forms;

- Membership applications and renewals;
- Council applications;
- Recordings of online interactive content.

British Exploring Society may also collect personal information or sensitive personal information when resources are downloaded from the website, a survey is completed or if we are contacted by email. In addition, we use software to identify which areas of our site are visited most frequently. This helps us to understand how our website is being used so that we can make it more useful for visitors.

What is personal and sensitive personal information collected used for

Information we collect may be used to:

- Process applications,
- Establish identity;
- Process payments;
- Keep a record of essential contact details;
- Enact any operational procedures including evacuations, support evaluation and offer web-based content;
- Engage staff;
- Pay staff;
- Maintain personnel records;
- Engage volunteers and make any appropriate arrangements for them;
- Process donation pledges;
- Promote British Exploring Society;
- Respond to requests for information;
- Provide newsletters or details of events, contact stakeholders with information about our work, events, campaigns and activities, or any other features of British Exploring Society;
- For our business purposes, such as data analysis, audits, fraud monitoring and prevention, enhancing, improving or modifying our services, identifying usage trends, determining the effectiveness of campaigns and operating and expanding our charitable activities;
- As we consider to be necessary or appropriate: (1) under applicable law, including laws outside any specific country of residence; (2) to comply with legal process; (3) to respond to requests from public and government authorities including public and government authorities outside any specific country of residence; (4) to enforce our terms and conditions; (5) to protect our operations; (f) to protect our rights, privacy, safety or property and/or that of our stakeholders; and (6) to allow us to pursue available remedies or limit the damages that we may sustain;
- To contribute to our Archive,

Who is information shared with

At times we need to share the personal and sensitive information with the data subject, and also with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act. This means that any Data to be shared will be:

- Processed fairly and lawfully;
- Processed for limited, defined purposes and in an appropriate way;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept longer than necessary for the purpose;
- Processed in line with a data subject's rights;

- Secure;
- Not transferred to people or organisations without adequate protection.

The following is a list of the types of organisations with whom we may need to share some of the personal or sensitive information we process for one or more reasons. Where necessary we share information with:

- Family, associates or representatives of the person whose personal data we are processing;
- Employees;
- Volunteers;
- Partners;
- Trustees;
- Third party service providers including emergency services;
- Current, past and prospective employers;
- Healthcare, social and welfare organisations;
- Statutory bodies including HMRC;
- Providers of goods and services;
- Educator and examining bodies;
- Financial organisations;
- Employment and recruitment agencies;
- Survey and research organisations;
- Business associates and professional advisers;
- Police forces;
- Other voluntary and charitable organisations.

Compliance

A failure in data protection could lead to investigations and enforcement notices from the Information Commissioners office. Staff and volunteers who are found to be in breach of this policy will be subject of a disciplinary action which may result in dismissal (for staff) or being barred from future volunteering (volunteers). Breaches could also lead to criminal prosecution.

When in doubt on the provisions of this policy, refer to a line manager.

Retention of Data and Data Destruction Schedule

Guidelines for retention of records are given in Annex A.

No documents are stored for longer than necessary. Documents containing personal and sensitive data are disposed of securely in accordance with Data Protection principles.

Paper-based data will be shredded. External shredding services handling personal and sensitive data will provide a Chain of Custody, be verified as secure and will be required to provide a Certificate of Destruction.

Wherever possible information will be stored in an electronic format, as long as an original[2] copy is capable of being produced from the electronic copy. This implies a high standard of legibility for electronic images such that no ambiguity of interpretation is introduced that does not derive from the original.

[2] 'Original' means a copy which is equivalent in every relevant legal respect in its characteristics to the original document no matter how many times removed it is from an original paper document.

Digital data is deleted from our system according to the schedule in annex A. Our first obligation is to put data 'beyond use'. We then commit to permanent deletion of the data as soon as possible. Deleted data are retained for a month post-deletion, accessible only by our Administrator, and are then permanently deleted. No deleted records are retained on individual PCs.

We will de-identify or 'redact' any information sources kept for use beyond our retention schedule for the purposes of analysis/planning/to provide trend data. Such information use is likely to include incidents, demographic data, medical information, campaign information.

The only other sources of personal and sensitive data to be retained beyond the schedule below are those which are added to the Archive, which is a permanent record.

British Exploring Society will destroy data on an annual cycle, within the calendar year of a due destruction date for any particular item.

ANNEX A - DATA RETENTION SCHEDULE

RECORD	RETENTION PERIOD	NOTES
HR RECORDS		
Personnel Files – Leavers	Normally 12 months after departure	Personnel files **must** be destroyed a maximum of 6 years after employment ceases. Any files held for longer than 12 months post-departure need a file note specifying the reason to hold them for longer.
Images of staff, trustees and volunteers	Held in perpetuity (unless consent withdrawn or withheld)	Some images held as 'closed' files on the archive as we cannot secure consent or we deem them sufficiently sensitive to be unsuitable for open distribution (e.g. via our website)
Volunteer assessment files	1 year absolute maximum (if unsuccessful) or 12 months after departure	Personnel files **must** be destroyed a maximum of 6 years after employment ceases. Any files held for longer than 12 months post-departure will need a file note specifying the reason to hold them for longer.
OPERATIONS		
Duty Operations Team Communications Log	For 6 full years after expedition period is over, or until all participants are 21, if this is longer*	Unless on-going live/claims issues denote valid reason for retention *which will be designated against the records*
Correspondence	No longer than is necessary for the lawful purpose for which such personal data was processed.*	Unless explicitly authorised for retention in the archive *Correspondence remains the property of the author, not the recipient
Application forms and interview notes for unsuccessful candidates	1 year absolute maximum	
CVs of unsuccessful candidates	I year absolute maximum	Unless consent secured from candidate for CV to be held on record for consideration for other roles. Keep email consent on file
Redundancy details, payments, calculations	6 years from date of redundancy	Do not move to archive
Disciplinary records	As long as has been agreed in writing to the employee	Do not move to archive
Appraisal records	5 years, destroy on rolling basis	Do not move to archive
Employee/consultant time sheets	2 years	Do not move to archive
Pensions scheme investment policies	12 years from the ending of any	Do not move to archive

	benefit payable under the policy	
Money Purchase details	6 years after transfer or value taken	Do not move to archive
PAYROLL		
Salary records/payroll records SSP records/ certificates	6 years	Do not move to archive
SSP records/ certificates	3 years after the end of the tax year	Do not move to archive
SMP records/ certificates	3 years after the end of the tax year	Do not move to archive
HEALTH & SAFETY		
Accident books, records	3 years after last entry	Do not move to archive
Incident Reports	For 6 full years after expedition period is over, or until all participants are 21, if this is longer*	Unless on-going live/claims issues denote valid reason for retention *which will be designated against the records*
Insurance certificates Insurance policies	Retain for 6 years or until all insured parties reach age 21.	Do not move to archive There is no specific statutory period for making a claim under an insurance or reinsurance contract. Insurance contracts are subject to the normal limitation period for causes of action founded on breach of contract (6 years from the date on which the cause of action accrues). Personal injury claims are limited to 3 years (but this only starts when a child reaches 18, even if an injury occurred when they were 15) The statutory period for a claim of negligence is 6 years. A claim for breach of trust must be brought within 6 years The 'limitation period' commences when the last fact which could give rise to the claim was in existence
Health & Safety Assessments	Permanently	
GOVERNANCE		
Trust deeds, Articles of Association	Permanently Most up to date version of Articles	Older versions of articles may move to Archive
Minutes of Trustee meetings	10 years	May move to archive subsequently with consent
External partnership/ forum meetings, minutes and papers	1 year	

FINANCIAL INFORMATION		
Accounting Records	6 years after end of tax year	Do not move to archive
Income Tax and NI returns	3 years	Do not move to archive
Funding information	6 years after end of tax year	Do not move to archive
Contracts	Life of contract + 6 years	Do not move to archive
DBS/CRB		
External disclosures	6 months only	Unless a dispute is raised
Internal disclosures	6 months only	Unless a dispute is raised
Records relating to international criminal records checks	6 months only	Unless a dispute is raised
CLIENTS		
Personal contact details Medical forms Application and Contractual agreements	Until applicant is 21, if the explorer is less than 18 when participating on expedition, or 6 full years after expedition period is over *	*Personal injury claims are limited to 3 years (starting when a child is 18) The statutory period for a claim of negligence is 6 years
Next Of Kin details if separate from YE application	Destroy within 12 months of return from expedition	Unless on-going live/claims issues denote valid reason for retention which will be designated against the records
Confidential expedition reports Fire Journals Any project materials identifying individuals	Destroy within 12 months of return from expedition	Unless consent secured for archiving and publication
Images	Held in perpetuity both for general use and for archive	Unless consent withdrawn or withheld Some images for archive not released – under-18 nudity, for example – caution should be used for all images where consent cannot be confirmed
Recordings from online activities – Footage containing Explorers	6 years or until participants reach age 21	
Recordings from online activities – Footage containing staff only	2 years	For training and development purposes. May be moved to archive after 2 years with consent of Session Leader.
MARKETING and MEMBERSHIP		

Membership contact details	For lifetime of member, with consent	Details checked with data owner for accuracy at least every 2 years
Email lists: Leaders Newsletter School talks	Opt-out as best-practice provided for every communication – no data scrub currently	Limited personal data Review if more data collected