Retention and Disposal Policy

The John Muir Trust's Retention and Disposal Policy clarifies how personal data the Trust receives and processes, is retained, and disposed of, in line with UK General Data Protection Regulation (UK GDPR) and other regulatory legislation.

This Policy is supplemented by a detailed retention schedule ('the Schedule') which sets out the appropriate retention periods for each material category of data held by us.

This Policy applies to all of our employees, contractors, volunteers, and Trustees who must familiarise themselves with this policy and comply with it at all times.

All those to whom this Policy applies are referred to as you and your in this Policy and references to we, us, our, or the Trust refers to John Muir Trust.

This Policy (and the accompanying Schedule) applies to all data that we hold or have control over (including data held by a third party on our behalf). This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, audio and video recordings, CCTV recordings and data on other removable or other media. It applies to both personal data and non-personal data. In this Policy we refer to this information and these records collectively as Data.

Personal data is information that relates to an identified or identifiable individual, whether directly or indirectly. Personal data can be as simple as a name or a number or other identifiers such as an IP address or a cookie identifier, or more complicated, for example, a combination of significant criteria (eg age, occupation, place of residence), making a data subject identifiable.

Personal data may also include special categories of personal data or criminal conviction and offences data. These are more sensitive, and these may only be processed in more limited circumstances.

This Policy does not form part of any contract that we have with you (e.g. contract of employment or contract for services) and it may be amended by us at any time.

Any breach of this Policy by you will be taken seriously and may result in disciplinary action and/or termination of our contract with you.

Any questions about the operation of this Policy or any concerns that the Policy has not followed should be referred in the first instance to the GDPR Support Team (jmt.privacy@johnmuirtrust.org).

This Policy is an internal document and cannot be shared with third parties, service users or

regulators without the prior permission of the GDPR Support Team (jmt.privacy@johnmuirtrust.org).

The Trust securely stores data in numerous locations across the organisation, including servers, (in house and externally), email accounts, workstations, backups, video and audio, and paper files.

Retention of data

Personal and special category data will only be retained as long as necessary for the purpose of processing, or as required by our legal or regulatory obligations.

We only collect personal or special category data we actually need for our specified purposes.

During the retention period, the data controller will regularly review data to ensure it is kept up to date and is being processed in line with the legal grounds for processing.

We do our utmost to keep personal information which we hold up to date, but if you think that we are holding information which is inaccurate then please contact the GDPR Support Team (jmt.privacy@johnmuirtrust.org).

Disposable information

Disposable information consists of data that may be discarded or deleted at the discretion of the user once it has served its temporary useful purpose, and/or data and its deletion which been agreed with the end user, that may be safely destroyed because it is not a formal or official record, as defined by this policy and the Record Retention Schedule. Examples may include:

- Duplicates of originals that have not been annotated.
- Preliminary drafts of letters, memoranda, reports, worksheets, and informal notes that do not represent significant steps or decisions in the preparation of an official record.
- Books, periodicals, manuals, training binders, and other printed materials obtained from sources outside of the Trust and retained primarily for reference purposes.
- Spam and junk mail.

The Schedule will not set out retention periods for disposable information. This type of data should only be retained as long as it is needed for business purposes. Once it no longer has any business purpose or value it should be securely disposed of.

Storage of data

Personal data should not be kept for longer than necessary, suggested retention periods are outline in the Schedule below. Stored data should be periodically reviewed and eased or anonymised wherever possible.

Electronic

Personal data should be stored in secure folders with restricted access on the server. Staff can request secure folders from the Business Support Manager. Where there is a requirement to share personal data the document(s) should be password protected before being sent my email to only those with a legal purpose for accessing the data. The password for the document should be shared separately either in a separate email or on a different platform (e.g. Microsoft Teams).

Access to mailboxes should be restricted to authorised users.

Mobile devices

Personal data must only ever be stored on mobile devices provided for this purpose by the Trust. Mobile devices should be password-protected and encrypted using encryption software which meets current standards to protect personal data - password protection alone is insufficient when the mobile device is handling personal data which if lost could cause damage or distress to individuals. Access to the device should be locked if an incorrect password is input too many times. The device should automatically lock if inactive for a period of time.

Mobile devices should be equipped with software to enable the device to be tracked and remotely wiped of data in the event of loss/theft.

Personal data must NEVER be stored on or transferred to staff members' personal devices such as mobile telephones, tablet or laptop computers, home computers, memory sticks, etc.

Physical documents

Physical copies of personal data should generally be scanned and saved securely. The physical copy should be shredded where there is not a legally reason to retain it (e.g. it is a formal or official record). If it is necessary to retain a physical copy of the data, this should be stored in lockable storage with restricted access, staff may request lockable storage from the Business Support Manager.

Disposal of data

You are responsible for the continuing process of identifying the data that has met its required retention period and supervising its destruction, always with prior discussion with your Line Manager. The destruction of confidential, financial, and employee-related hard copy data must be conducted by shredding if possible. Non-confidential data may be destroyed by recycling. The destruction of electronic data must be co-ordinated with the Business Support Manager.

Anonymisation of data

Data will be held in line with the below retention periods. At the end of that period, data will be deleted unless the records are required for archiving, research or statistical purposes, in which case the data will be anonymised in a timely manner.

If anonymised, this will be by:

- erasing unique identifiers within the data
- deleting all information that identify the data subject
- separating personal data from non-identifying information

In some cases, no action will be required if data cannot be allocated to an identifiable person at the end of the retention period.

Exemptions

The requirements of this Policy and the Schedule do not apply in the following circumstances (each an **Exemption**):

1. **Legal / regulatory requirements.** The Schedule takes into account legal and regulatory requirements. However, these requirements may change over time or new requirements may apply and must be complied with. In the event that any new requirements are introduced then we will try to update this Policy promptly in light of those.

2. **Litigation.** If we ever need to take or defend actual, threatened, contemplated or pending legal proceedings, we may need to retain certain Data for longer than set out in the Schedule. This exemption applies as soon as legal proceedings are contemplated or anticipated.

3. **Insurance claims.** Once a claim or potential claim is notified to our insurers, the Data relating to that claim should be retained until the insurer agrees otherwise, even if retention goes beyond the relevant time limit(s) in the Schedule.

4. **Data which is in the subject of an investigation.** Where a request for information is received from a regulator or investigatory body (e.g OSCR, Companies House, the Information Commissioner's Office), all documents and information falling within the scope of the request must be retained while our obligations in respect of the request are determined. This exception always supersedes the retention periods set out in the Schedule.

Purpose of this Schedule

The Schedule describes the broad categories of Data held by us and the appropriate retention period for each of those categories in light of the relevant legal and regulatory requirements, relevant time limits for bringing claims, good practice and our charitable objectives. This Schedule is a non-exhaustive list of the categories of Data that we hold and will be kept under review.

Category of Data	**Period for which the Trust is to hold the Data for**
Human Resources	
Pre-employment enquiries/applications/notes/letters/references	Unsuccessful candidate: 6 months from the date we inform the candidate that they have been unsuccessful. Successful candidate: 7 years from the date the person's employment ceases or engagement with us ends. The Trust does not retain speculative enquires or CVs. Special Category data (e.g. data about ethnicity, sexual orientation, religious beliefs etc.) may be retained indefinitely provided it is aggregated and anonymised. Criminal offence data such as a DBS check will not be kept for any longer than is necessary and at most retained for the same period as other pre-employment enquires.
Personnel records in general (including special category data, grievance and disciplinary records, annual leave records, appraisal records, occupational health/doctor's reports, death benefit nomination and revocation forms, and records relating to resignation, termination, and retirement).	7 years from the date the person's employment or engagement with us ends. Special Category information may be retained indefinitely provided it is aggregated and anonymised. Employee survey responses may be retained indefinitely provided the responses are aggregated and anonymised.
Payroll and benefits records (including bonuses, expenses, overtime, benefits in kind, travel and subsistence).	7 years from the date the person's employment with us ceases.
Statutory sick pay records, calculations, certificates, self-certificates.	7 years from the date the person's employment with us ceases.
Family records (ie statutory maternity, paternity, adoption and parental leave pay).	4 years after the end of the tax year in which the relevant pay period ends.

Category of Data	Period for which the Trust is to hold the Data for
Pension plans and retirement records	Permanent
Salary schedules; ranges for each job description	3 years
Employment references provided to third parties.	7 years from the date the person's employment with us ceases.
Volunteer records	Duration of placement + 7 years
Health and safety records (including training and compliance records).	3 years for general records from the date after the person's employment with us ceases. Permanently for records relating to hazardous substances.
Miscellaneous contact information	Delete once there is no longer a requirement to hold such information
Documents relating to litigation or potential litigation	Until matter is concluded plus 7 years
Hazardous material exposures	30 years
Injury and Illness Incident Reports (RIDDOR)	5 years
Databases for mailing lists/distribution	Reviewed annually, delete out of date information
Legal Documents	
Contract with customers, suppliers or agents, licensing agreements, rental hire purchase agreements, indemnities and guarantees and other agreements or contracts	Agreements executed as simple contracts: 7 years from expiry/termination. Agreements executed as deeds: 13 years from expiry/termination.
Construction documents	Permanent
Fixed Asset Records	Permanent
Application for charitable and/or tax-exempt status	Permanent
Insurance claims/ applications	Permanent
Insurance disbursements and denials	Permanent
Insurance contracts and policies (Directors and Officers, General Liability, Property, Workers' Compensation)	Permanent
Leases	7 years after expiration

Category of Data	Period for which the Trust is to hold the Data for
Property/buildings documentation (including loan and mortgage contracts, title deeds)	Permanent
Warranties	Duration of warranty + 7 years
Records relating to potential, or actual, legal proceedings	Conclusion of any tribunal or litigation proceedings + 7 years
Governance	
Resolutions	Permanent
Audit and review workpapers	5 years from the end of the period in which the audit or review was concluded
OSCR filings	5 years from date of filing
Trustee minutes of meetings and decisions made as resolutions in writing.	Minimum 10 years from the date of the meeting or from the date of passing a resolution in writing
Minutes of general meetings and members' resolutions passed other than at a general meeting.	Minimum 10 years after the date of the meeting/resolution/decision
Finance	
Sales and purchase records	7 years
Records of financial donations	7 years
Accounts Payable and Receivables ledgers and schedules	7 years
Annual audit reports and financial statements	Permanent
Annual plans and budgets	5 years and then anonymised
Bank statements, cancelled cheques, deposit slips	Minimum of 7 years
Business expense records	7 years
Cash/cheque receipts	7 years
Electronic fund transfer documents	7 years
Employee expense reports	7 years
General ledgers	Permanent
Journal entries	7 years
Invoices	7 years

Category of Data	Period for which the Trust is to hold the Data for
Petty cash vouchers	7 years
Tax records	Minimum 7 years
Filings of fees paid to professionals	7 years
Environmental studies	Permanent
Gift Aid Declarations.	6 years after last donation
Legacy pledges.	10 years after supporter's death is notified
Other Data All other contacts who engage with the Trust	
Service user data. For example, service user file notes, records of meetings with service users, records of referrals to third party service providers.	7 years after the date which the service user ceases to use the Trust's services.
Details of service user complaints. For example, correspondence.	7 years from the date their complaint is received.
General correspondence from service users.	7 years from receipt of general correspondence.
CCTV images of service users.	40 days from the date of the recording unless a crime is reported to the police and the police require additional time to collect the images.

QUESTIONS OR COMPLAINTS

In addition, and where granted by applicable law, you may have the right to lodge a complaint with a competent data protection authority.

If you would like to make a request to access, review, correct, delete or port the personal data we have collected about you, to assert a right with regard to your personal data, or to discuss how we process your personal data, contact us using the information at the end of this Retention Policy.

To help protect your privacy and security, we will take reasonable steps to verify your identity before granting you access to your personal data. We will make reasonable attempts to promptly investigate, comply with, or otherwise respond to your requests as may be required by applicable law. Depending upon the circumstances and the request, we may not be permitted to provide access to personal data or otherwise fully comply with your request; for example, where producing your information may reveal the identity of someone else. We reserve the right to charge an appropriate fee for complying with your request where allowed by applicable law, and/or to deny your requests where, in the Trust's discretion, they may be unfounded, excessive, or otherwise unacceptable under applicable law.

It is the responsibility of our GDPR Support Team to oversee compliance with this policy. Should you have any questions regarding this policy, please contact the GDPR Support Team (jmt.privacy@johnmuirtrust.org).

John Muir Trust
Tower House
Station Road
Pitlochry
PH16 5AN

If you are not satisfied with our response, please contact the ICO for the UK or Scotland:

The Information Commissioner's Office - Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT

Telephone: 0303 123 1115
Email: Scotland@ico.org.uk

Information Commissioner's Office – UK
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ico.org.uk/livechat, or call our helpline on 0303 123 1113.