



Data Retention Policy, Schedule & Action Plan

Document Control:

Version	Date Written	Authors	Date Ratified	Judgement of controls/Amendments
0.1	14/04/22	K Brownlee		Good
0.2	22/06/2023	S.Gillam	22/11/2023	Standardising format

Contents

1. Charity Statements:	3
Mission:.....	3
Charity Objectives:	3
Our Values:.....	3
Statement of public benefit:	3
2. Purpose, Scope and Users:.....	3
3. Reference documents:	4
4. Exceptions	4
5. Destruction of Data	4
6. Breach, Enforcement and Compliance	4
7. Document Disposal	5
8. Destruction Method.....	5
9. Validity and document management	6
10. Data Retention Schedule	7
11. Wiltshire Treehouse Data Retention Schedule – ACTION PLAN	13

1. Charity Statements:

Statement of public benefit:

Wiltshire Treehouse is for the benefit of bereaved children, young people, and their families, living/educated within Swindon & Wiltshire.

Mission:

Wiltshire Treehouse wants to see a world where every bereaved child and young person can receive guidance and support to help them through their grieving process. We will enable those in our local communities to develop the coping strategies, skills, and confidence they need to thrive.

Charity Objectives:

Provide high quality, relevant bereavement support and guidance to children, young people & their families.

Improve the initial experience of a child bereavement through training and awareness raising.

Secure the continuity of our organisation, ensuring a future of child specific bereavement support.

Be proud of the charity, a great place to work and achieve.

Our Values:

Growth – Providing a safe space for personal development.

Respect – Beneficiaries, volunteers, and staff are treated with respect and dignity within their journey with the charity.

Inclusivity – Services and support available to the whole community.

Empowerment – Working with beneficiaries to enable change on their terms.

Friendly – Open and welcoming.

2. Purpose, Scope and Users:

Data protection law does not set retention periods. Instead, there is a storage limitation principle which means that organisations should not keep data for longer than they need it.

Having taken into consideration factors such as the purpose for which data was originally collected and any laws or guidelines that must be adhered to, Wiltshire Treehouse have compiled this Data Retention Policy and Schedule.

This document adheres to Data Protection principles that state that data stored should be 1) adequate, relevant and not excessive for the purpose(s) for which they are held 2) accurate and up to date 3) only kept for as long as is necessary (*Information Commissioner's Office, 2021*).

This schedule should be read in conjunction with the Wiltshire Treehouse Data Protection Policy.

This document applies to all departments within Wiltshire Treehouse and all personnel, both paid and voluntary.

The format that the information is held in is not relevant. If personal data exists in any form, in electronic or paper-based media, it is covered. Paper based records such as files; card indexes and photographs are also covered. Paper-based data should be securely disposed of regularly, and information uploaded to the electronic system where appropriate.

3. Reference documents:

- Records Management Code of Practice for Health and Social Care [Records Management Code of Practice - NHS Transformation Directorate \(england.nhs.uk\)](https://www.england.nhs.uk/records-management-code-of-practice/)
- Wiltshire Treehouse Data Protection Policy
- [Child protection records retention and storage guidelines \(nspcc.org.uk\)](https://www.nspcc.org.uk/child-protection-records-retention-and-storage-guidelines/)
- [Child protection records retention and storage \(icmec.org\)](https://www.icmec.org/child-protection-records-retention-and-storage/)
- [Principle \(e\): Storage limitation | ICO](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/principle-e/)
- [IRMS Schools Toolkit - Information and Records Management Society](https://www.irmschools.org/)

4. Exceptions

As an exemption, retention periods within the Data Retention Policy can be prolonged in cases such as:

- Legal holds which can take many forms. Records shall not be destroyed if there is a known process or an expectation that records will be needed for a future legal process. This may include national or local inquiries, criminal Bereavement Services Data Retention Policy Version 1 April 2022 3 investigation, and expected cases of litigation or records that may be requested under subject access.
- When exercising legal rights in cases of lawsuits or similar court proceedings recognised under local law.

5. Destruction of Data

The Service and/or Business Directors of Wiltshire Treehouse shall be responsible for the review of all service data on an annual basis, to decide whether to destroy or delete any data once the purpose for which those documents were created is no longer relevant (see Appendix for the retention schedule).

Once the decision is made to dispose according to the Retention Schedule, the data should be deleted, shredded or otherwise destroyed to a degree equivalent to their value to others and their level of confidentiality. The method of disposal may vary and is dependent upon the nature of the document. For example, any documents that contain sensitive or confidential information (and particularly sensitive personal data) must be disposed of as confidential waste and be subject to secure electronic deletion; some feedback documents with no personal data may only warrant inhouse shredding.

Directors shall oversee the performance of the tasks relevant for the information destruction in an appropriate way. The specific deletion or destruction process may be carried out either by an employee or by an internal or external service provider that is contracted for this purpose.

Any applicable general provisions under relevant data protection laws and the Wiltshire Treehouse Data Protection Policy shall be complied with.

6. Breach, Enforcement and Compliance

Wiltshire Treehouse Directors are the appointed persons with responsibility for Data Protection (overseen by the board of trustees). They shall ensure that this policy is complied with. It is also their responsibility to assist with enquiries from any local data protection or governmental authority.

Any suspicion of a breach of this Policy must be reported immediately to the Directors. In an instance where a Director is suspected to be responsible of a breach it is appropriate to report this directory to the Chair of Trustees.

All instances of suspected breaches of the Policy shall be investigated and action taken as appropriate. Failure to comply with this Policy may result in adverse consequences, including, but not limited to, loss of service user confidence, litigation, damage to Wiltshire Treehouse's reputation, personal injury, harm or loss.

Non-compliance with this Policy by permanent, temporary or contract employees, volunteers or any consultants or third parties, who have been granted access to the Charity's premises or information, may result in disciplinary proceedings or termination of employment or contract. Such noncompliance may also lead to legal action against the parties involved in such activities.

7. Document Disposal

Records which shall be routinely destroyed, according to the timescales set in the Data Retention Schedule, unless subject to an on-going legal or regulatory inquiry, include the following:

- Referral forms
- Practitioner assessment notes
- Practitioner support session notes
- Practitioner support group or other event notes
- Liaison notes with other professionals
- Communications from the individual/family
- Creative work produced by children/families
- Notices of appointments and meetings, and other events including acceptances and apologies
- Requests for bereavement support information or advice – including but not limited to requests from parents, carers, professionals, and children
- Requests for ordinary information such as travel directions, rescheduling appointments
- Transmission documents such as letters, fax cover sheets, e-mail messages, compliments slips and similar items that accompany documents but do not add any value
- Message slips
- Superseded address list, distribution lists etc.
- Duplicate documents such as CC and FYI copies, unaltered drafts, screenshots, printouts or extracts from databases and day files
- Service user database (electronic) record In all cases, disposal is subject to any disclosure requirements which may exist in the context of litigation.
- Financial records, including but not limited to records from individual or corporate donations and payments for services (e.g. training)

8. Destruction Method

Level I documents are those that contain information that is of the highest security and confidentiality and those that include any personal data. These documents shall be disposed of as confidential waste (cross-cut shredded and incinerated) using an approved secure waste disposal firm and shall be subject to secure electronic deletion.

Disposal of the documents should include proof of destruction which must be logged with a Director.

Level II documents are proprietary documents that contain confidential information such as feedback forms, but which do not contain any personal data. The documents should be cross-cut shredded and then

placed into locked rubbish bins for collection by an approved disposal firm, and electronic documents will be subject to secure electronic deletion. Secure electronic deletion refers to the permanent or irretrievable deletion of electronic record.

9. Validity and document management

This document is valid as of its review date.

The owner of this document are the Directors in conjunction with the board of trustees who must review and, where necessary, update the document at least once a year.

10.Data Retention Schedule

	Data	Data Type	Period of retention	Justification	Notes
1	<p>Client engagement – from point of initial contact to closing of file.</p> <p>To include (but not limited to) referral form, consent forms and all contact notes.</p>	Personal and sensitive data	<p>Until client’s 25th or 26th birthday (see Notes)</p> <p>Action at end of period: Level 1 destruction</p>	Adopted from guidelines set out in Records Management Code of Practice for Health and Social Care 2021	<p>Basic health and social care retention requirement is to retain until 25th birthday or if the patient was 17 at the conclusion of the treatment (in the Charity, support), until their 26th birthday. Check for any other involvements that could extend the retention. All must be reviewed prior to destruction taking into account any serious incident retentions, safeguarding notifications/records or on-going legal action. If in doubt, seek advice from the Information Commissioner (ICO).</p> <p>This Policy should be followed in the same way for electronic records as for paper records with a meta data log being kept of the records destroyed.</p> <p>Annual April compliance check</p>
2.	Safeguarding concerns about a young person - regardless of whether the concerns are shared	Personal and Sensitive data	<p>7 years after the last contact with the child and their family.</p> <p>Action at end of period: Level 1 destruction</p>	All data about safeguarding concerns potentially form part of an important story that may be needed	Annual April compliance check

	with the police or children's social care			retrospectively for many years. Required for evidence requests from statutory agencies	
3	Staff/volunteer enquiries and applications	Personal data	1 year after last contact (e.g. enquiry, interview, etc). Action at end of period: If unsuccessful - level 1 destruction If successful, records will be added to the personnel file.	To keep them informed of their joining status. To allow time for any claims bought against us by unsuccessful applicants.	Annual April compliance check
4	Vetting	Personal and sensitive data – Disclosure Certificate	6 months if there is a dispute over the record. Action at end of period: Level 1 destruction NOTE: No copies to be kept if no dispute – but it is reasonable to keep the date the check was completed, the level and type of check, the reference number of the certificate and the decision made about whether the person was accepted/hired.	In line with DBS, Access NI and Disclosure Scotland Code of Practice	Annual April compliance check

5	Staff and volunteer personnel files	Personal and sensitive data	<p>6 years from termination, unless there is a safeguarding allegation (see point 6 below).</p> <p>Action at end of period: Level 1 destruction</p>	For purposes of providing references and data requested for evidence from statutory agencies	Annual April compliance check
6	Safeguarding – Adult perpetrator (volunteers and paid staff)	Personal and Sensitive data	<p>Records should be kept in the personnel file at least until the individual reaches their normal retirement age or for 10 years – whichever is longer (IRMS, 2019; Department for Education, 2021).</p> <p>In the event that the allegation is actually disproved or is found to have been mis-recorded in the first place, the record will include a statement that the data subject has been exonerated.</p> <p>Data will be kept for the same amount of time regardless of whether the allegations were unfounded.</p>	Required for evidence requests from statutory agencies, future reference requests and clarification about information disclosed as part of vetting or clearance checks	Annual April compliance check

			<p>However, if allegations are found to be malicious records will be destroyed immediately.</p> <p>Action at end of period: Level 1 destruction</p>		
7	Safeguarding – Young person perpetrator (under 18)	Personal and Sensitive data	<p>Young Person – Until child reaches 25yrs old.</p> <p>In the event that the allegation is actually disproved or is found to have been mis-recorded in the first place, the record will include a statement that the data subject has been exonerated.</p> <p>Data will be kept for the same amount of time regardless of whether the allegations were unfounded.</p> <p>However, if allegations are found to be malicious records will be destroyed immediately.</p> <p>Action at end of period: Level 1 destruction</p>	Required for evidence requests from statutory agencies	Annual April compliance check

	Incident – personal injury (including sexual abuse/psychological damage). Including accident and incident books.	Personal and Sensitive data	4 years after incident, or 4 years after alleged victim turns 18 if later. Action at end of period: Level 1 destruction	Fight a case – Limitation act 1980	Annual April compliance check
	Incident – not involving personal injury Including accident and incident books.	Personal and Sensitive data	7 years after incident, or 7 years after alleged victim turns 18 if later. Action at end of period: Level 1 destruction	Fight a case – Limitation act 1980	Annual April compliance check
	Publicity material - Case studies and photographs	Personal data	3 years after submission Action at end of period: Level 1 destruction	Required for the team to ascertain if these items still accurately reflect the charity and its aims	Annual April compliance check
	Individual Givers – personal donations	Personal data	5 years post last donation. Action at end of period: Level 1 destruction	To keep an individual informed of their donation and other fundraising campaigns	Annual April compliance check
	Individual Givers – gift aid declaration	Personal data	6 years after the end of the year or accounting period that includes the last donation. Action at end of period: Level 1 destruction	HMRC Tax Audit	Annual April compliance check

Individual Givers – direct debit mandate	Personal data	6 years after the end of the year or accounting period that includes the last Direct Debit. Action at end of period: Level 1 destruction	As proof of Direct Debit Instruction (DDI) and to assist in claims against that DDI	Annual April compliance check
Users of paid services – e.g. training participants	Personal data	12mths, unless permission received to keep their details on file. Action at end of period: Level 1 destruction	To report on projects, donations and maintain a record of partner donors.	Annual April compliance check
Partnerships – Including operational and fundraising partners	Personal data	3 years Action at end of period: Level 1 destruction	To report on projects, donations and maintain a record of partner donors.	Annual April compliance check
Fundraising events - attendees	Personal data	12 months Action at end of period: Level 1 destruction	To re-invite the guests to the same event in the following year.	Annual April compliance check

Notes:

Safeguarding concerns relate to those where a referral to statutory services could be required (police or social care). Even where concerns are not reported, they should be kept as they may provide an important piece of the puzzle if an investigation is instigated.

Other concerns, such as those around self harm or suicidal thoughts do not need to be kept – if an investigation was launched around these circumstances it would likely be a child safeguarding practice review, which would focus on the 12 months leading up to the incident (this period would be covered by the standard retention period of 12months).

Organisations must keep any records that could be needed by an official inquiry (for example the Independent Inquiry into Child Sexual Abuse (IICSA) (IICSA, 2018). Inquiries will issue directions for records to be retained and these must be followed.

Where there are legal proceedings we will seek legal advice about how long to retain records.

11. Wiltshire Treehouse Data Retention Schedule – ACTION PLAN

Action	Who	Priority	Completed?
Add to training participant survey: i) Would they like us to keep their email address for marketing purposes (they can unsubscribe at any time)	Gemma Stanley, Administrator	1 Target: end of Oct 22	
Add comment to referral forms, consent forms and Eventbrite forms saying individuals can contact us for a full copy of our Data Protection Policy & Data Retention Policy & Schedule	Gemma Stanley, Administrator	2 Target: end of Oct 22	
Update privacy notice on website	Gemma Stanley, Administrator	3 Target: end of Oct 22	
Align data protection policy, safeguarding policy & privacy notice.	Kath Brownlee, Service Director	4 Target: end of Oct 22	Complete Aug 22
Implement process to identify data needing destruction	Kath Brownlee, Service Director & Gemma Stanley, Administrator	5 Target: end of Dec 22	
Implement a system of log keeping for data destruction	Kath Brownlee, Service Director	6 Target: end of Dec 22	
Create a compliance checklist/system.	Kath Brownlee, Service Director & Gemma Stanley, Administrator	7 Target: end of Dec 22	
Maintain a spreadsheet of those who have given consent for us to hold their email address for marketing purposes (they can unsubscribe at any time). This could include families, professionals and supporters	Gemma Stanley, Administrator	8 Target: end of Dec 22	
Source a suitable company to destroy our secure waste		9 Target: Dec 2023	