The Knapp Foundation
Registered Charity Number: 1200294

Data Retention Policy

Purpose

1. To ensure that the Foundation keeps data (especially Personal Data) no longer than it needs to, and that Right to be Forgotten procedures are in place. This policy will be reviewed every three years or when there has been a change in legislation.

2. To ensure that data relating to the Foundation's working are securely protected from accidental loss, equipment failure, or theft. The Foundation recognises that there is a distinction between ordinary working data or personal data, and data relating to publications, research etc. Working and Personal data are covered under §§3–5 below: research data are covered under §6.

Personal Data

3. Personal Data (ie data which names an individual or from which an individual maybe named) may be:

Employee data;

Contractor data;

Financial data;

Data related to incidents;

Complaints; and

Any other data which might contain personal details

Data purpose and retention periods

4. **Appendix 1** sets out in detail how data may retained and disposed of. **Appendix 3** (taken from the website of the Information Commissioner's Office) gives details of a wide range of different documents and indicates how long they must be kept, and why. Its contents should be followed *ceteris paribus* by the Foundation and its employees. It covers the following headings:

i. Communications;
ii. Charity communication & Marketing;
iii. Charity functions;
iv. Governance;
v. Finance;
vi. HR;
vii. Legal;
viii. Regulatory (internal & external);
ix. Stakeholder engagement; and
x. Archives

Right to be forgotten

5. Individuals may apply to the Chairman to have information erased under the Right to be Forgotten. **See Appendix 2.**

Research Data

6. Research data are data or bodies of material stored electronically which relate to research streams and individual projects supported by the Foundation. This covers data to which individuals employed by, or participating in projects organised by, the Foundation hold copyright, or where copyright is held by the Foundation itself. These data are assets, either belonging to the Foundation, or held in custody electronically by the Foundation on behalf of the individuals with the right to assert copyright over them. They must therefore be kept safe.

All data held in this way, especially data that are subject to revision or change must be backed up regularly to a central, secure, and cloud-based source to which the responsible individual, and Director or at one other authorised individuals have access.

Data must be backed up daily in the case of work in progress, and monthly in the case of completed or finished work.

All necessary steps must be taken to protect any data that constitute an individual's or group's property or research materials.

This policy was agreed on…….

Appendix 1: Detailed provisions

Introduction and Scope

1. The aim of the Retention and Disposal Policy is to outline the Foundation's approach to managing the retention and secure disposal of our information in line with our business requirements and legal obligations. There are various pieces of legislation which outline retention requirements. These include, but are not limited to:

- Freedom of Information Act 2000 – including the Code of Practice Section 46 (FOIA)
- The UK General Data Protection Regulations (the UK GDPR)
- Data Protection Act 2018 (DPA 18)
- Public Records Act 1958 • Limitation Act 1980
- Inquiries Act 2005

2. The requirements outlined in this policy have been developed to provide a consistent approach to the retention and disposal of Foundation information. This policy applies to all physical and digital information, regardless of storage location.

Roles and Responsibilities

3. All Foundation staff are responsible for managing the information they create and receive as part of their normal daily business activities and should familiarise themselves with the Retention and Disposal Schedule.

Retention Periods

4. Foundation retention periods are driven by legislation and/or business need. If there is no legally defined retention period for corporate information it is the responsibility of the Chair to determine an appropriate retention period. There are defined retention periods for Foundation information to ensure it is kept for the appropriate length of time. Each retention period has three elements:

i. Trigger – the action which begins the retention period (e.g., 'End of Financial Year' or 'End of Employment')
ii. Retention period – the length of time the information will be kept
iii. Action – either 'review' or 'destroy'. If the action is 'review' the information must be reviewed to ensure it is no longer required before destruction.

5. Outcomes of a review may include: dispose; mark for permanent preservation; or agree a temporary extension to review again at a future date. If the action is 'destroy', this means the information can be destroyed without being reviewed in line with Trust procedure.

Retention and Disposal Schedule (Appendix 3)

1. The Retention and Disposal Schedule sets retention periods. Information must be kept for the length of time defined in the Schedule unless there is a legal requirement to destroy it sooner. The Schedule is arranged by function. Any proposed additions or changes to retention periods must be captured on this form and sent through to staff.

Weeding

2. Not all information we create has long-term value. The Retention and Disposal Schedule does not include redundant, obsolete or trivial (ROT) information. This should be destroyed periodically as part of routine housekeeping. Approval or sign-off to delete ROT information is not required. 'Weeding' does not apply to corporate records included in the Schedule, which should only be destroyed when they have reached the end of their retention period.

3. Information should be weeded for two reasons:

i. To ensure that we are not wasting money or space (either digital or physical) by storing ROT information.
ii. To make the process of reviewing and appraising records easier. Sifting through low value records makes this process more time-consuming.

4. Below are common examples of information which is usually of limited value once it is no longer in use, and can be weeded through housekeeping. This should not be seen as an exhaustive list:

- **Drafts** - Draft documents lose value and can become obsolete once a final version has been published. However, on some occasions where significant changes or deviation have taken place, a draft may be retained to show how the final decision was made.

- **Emails** - Once a conversation has reached a significant point, any earlier emails from this chain can be deleted.

- **Duplicates** – We should not retain any duplications. Duplications can lead to multiple versions of information which can cause confusion.

- **Research Material** – Whether developing policy or preparing to give advice, research material may be created or collected, such as notes or copies of guidance from external organisations. The value of this information decreases once the final version has been created.

5. Some information may be of importance for only a short period of time and then become redundant. This information should be weeded as soon as it is no longer required. Weeding should be done on a regular basis to ensure that clutter does not build up over time. It is up to staff to decide a reasonable schedule for housekeeping, based on their resources and the amount of information they generate. Weeding should cover all information the Foundation stores, paper or digital, regardless of the system it is held on. This includes personal drives and desktops.

Disposal

Review

6. When information has reached the end of its retention period it may need to be reviewed to ensure that it is no longer required. Information that has an action of 'destroy' on the Schedule can be disposed of securely without a review. Where possible, automated retention rules should be built into corporate systems.

7. When conducting a review, the following factors should be taken into account:

i. Is the information required to fulfil statutory or regulatory requirements?
ii. Is the information relevant to ongoing litigation / subject to a legal hold?
iii. Is the information the subject of an information request or relate to information recently disclosed in a response?
iv. Is retention required to evidence events in the case of a dispute?
v. Does the information fall under the selection criteria for permanent preservation and transfer to the National Archives?
vi. Is the information required for a Public Inquiry?
vii. Is there another demonstrable business need for retaining the information?

8. If the information is deemed to still be required, an extension of two years should be given, and the information needs to be reviewed again at the end of the extension. The retention period must not be extended indefinitely. Staff should discuss with Trustees if they still intend to keep the information after applying the two-year extension period.

Destruction

6. When records are no longer required by the Foundation and do not have archival value they should be securely destroyed. A record containing what has been destroyed, when it was destroyed and the individual who authorised the destruction should be created. Records should be destroyed with the level of security required by the confidentiality of their contents. For example, if records containing special category data or protectively marked papers have been shredded, the shredded paper should be handled securely and not dumped. Records awaiting destruction must be stored securely. Paper records should be placed into confidential waste bins and documents stored on electronic systems should be deleted, including back-ups. Deletions should be carried out by someone with appropriate access to the system from which they are

being deleted. Digital documents should be deleted and not overwritten. When information is destroyed, all copies of the information should be destroyed at the same time (both digital and physical). Information cannot be considered to have been completely destroyed unless all copies have been destroyed as well.

Permanent Preservation

7. Documents should be selected for permanent preservation if they meet the criteria specified in the Selection and Appraisal Methodology. Documents which have been marked for permanent preservation must not be destroyed. Any information which is selected for preservation should be clearly marked to ensure it is not destroyed accidentally.

Adopted by a meeting of the Trustees on 1st February 2023

Appendix 2: Right of Erasure

1. The data subject has the right to obtain from the Trustees the erasure of personal data concerning him or her without undue delay and the Trustees must erase personal data without undue delay if one of a number of conditions applies. “Undue delay” is considered to be about a month. The Foundation must also take reasonable steps to verify the person requesting erasure is actually the data subject.

2. An individual has the right to have their personal data erased if:

i. The personal data is no longer necessary for the purpose the Foundation originally collected or processed it.
ii. The Foundation is relying on an individual’s consent as the lawful basis for processing the data and that individual withdraws their consent.
iii. The Foundation is relying on legitimate interests as its justification for processing an individual’s data, the individual objects to this processing, and there is no overriding legitimate interest for the Foundation to continue with the processing.
iv. The Foundation is processing personal data for direct marketing purposes and the individual objects to this processing.
v. The Foundation processed an individual’s personal data unlawfully.
vi. The Foundation must erase personal data in order to comply with a legal ruling or obligation.
vii. The Foundation has processed a child’s personal data to offer their information society services.

3. However, the Foundation’s right to process someone’s data might override their right to be forgotten. Here are the reasons cited in the GDPR that trump the right to erasure:

i. The data is being used to exercise the right of freedom of expression and information.
ii. The data is being used to comply with a legal ruling or obligation.
iii. The data is being used to perform a task that is being carried out in the public interest or when exercising an organization’s official authority.
iv. The data being processed is necessary for public health purposes and serves in the public interest.
v. The data being processed is necessary to perform preventative or occupational medicine. This only applies when the data is being processed by a health professional who is subject to a legal obligation of professional secrecy.
vi. The data represents important information that serves the public interest, scientific research, historical research, or statistical purposes and where erasure of the data would likely to impair or halt progress towards the achievement that was the goal of the processing.
vii. The data is being used for the establishment of a legal defence or in the exercise of other legal claims.

4. Furthermore, the Foundation may request a “reasonable fee” or deny a request to erase personal data if the organization can justify that the request was unfounded or excessive.