Data Retention and Erasure Policy

Version No	V1.2
Approved on	7th November 2025
Previous Version No	V1.1
Approved on	29th November 2023
Signature of Chair of Trustees	*Julie Winyard*

Change Record

Date of Change:	Changed By:	Comments:

Under the Data Protection Act 2018 and the GDPR, all data, in all formats must only be kept for as long as is necessary.
Policy points are numbered. The numbering corresponds to explanations of ‘why?’ and ‘how?’ for each point further down the page.

What must I do?

1. ***MUST***: Information must be kept for the length of time defined in the Data Retention Schedule;
2. ***MUST***: The Data Retention Schedule must be reviewed on an annual basis;
3. ***MUST***: You must ensure that the information you manage is only known to an **appropriate audience;**
4. ***MUST***: All information in any format which we hold as a record of our activity must be **retained** after 'closure' in line with the Data Retention Schedule;
5. ***MUST***: Owners must regularly **review** information in line with Data Retention Schedule to make best use of the available storage space and to ensure that the data is not kept for longer than is necessary;
6. ***MUST***: We must **monitor** the success of the review process to maintain compliance with the UK GDPR and Data Protection Act 2018;
7. ***MUST***: You must manage trainee records in line with the Trainee and candidate record procedure
8. ***MUST***: You must follow the Email Retention Policy when storing **emails** as records
9. ***MUST***: We must ensure that the **facilities** available for storing and managing information meet legal requirements
10. ***MUST NOT***: You must not store business information on a **personal drive** or on equipment not provided by the Organisation
11. ***MUST***: All Information **Assets** identified on the Register must be associated with a retention period from the Data Retention Schedule
12. ***MUST***: The Data Retention Schedule must be reviewed for **changes** in legislation and the Organisation's business needs.
13. ***MUST:*** When archiving paper records, information on ownership, retention and indexing quality must be recorded.

Why must I do it?

- These measures ensure charity information, where appropriate to do so, is shared effectively to support efficient business processes and maintain effective service delivery to our trainees.
- Managing records in line with the best practice guidance fulfils duties under the section 46 Code of Practice on Records Management under the Freedom of Information Act 2000. Retention Guidelines are published so there is clear communication to customers over what information should still be available to them if they wish to make a request. To retain information too long or to destroy too soon leaves us open to criticisms on openness and transparency, and in some cases, compliance with the law.
- In order to comply with the Section 46 Code of Practice (see above) we must ensure that we are destroying all related information across all formats. For example, destroying a paper file on a project but keeping all the electronic documents about the project in a shared network folder can cause problems if a Freedom of Information request is received. The DPO assumes that as the paper file is destroyed then we do not hold any information and responds accordingly. We would then be in breach of the act.

How must I do it?

1. Employees are aware of best practice requirements and any guidance on use of specific systems through training and communications
2. You must ensure that paper files are accessible to authorised colleagues in your absence, by ensuring others know where to find keys to lockable storage areas. You must be aware of who information should be shared with, and ensure it is only shared with that audience. You must ensure that you save electronic information in a shared environment, but with appropriate access controls if the information has a restricted audience.

3. Follow the Retention Schedule within the ROPA and any superseding amendments made by the Organisation
4. Follow the Retention Schedule within the ROPA guidance and any superseding amendments made by the Organisation
5. Designated employees must gather performance data on activities within the scope of this policy for review by the Data Protection Officer and the Leadership Team
6. Follow the trainee and candidate records procedure and any superseding amendments made by the Organisation
7. Follow the managing email procedure and any superseding amendments made by the Organisation
8. The charity must approve and regularly review facilities such as systems and physical storage as appropriate against security requirements in Data Protection Law, and all employees must help maintain security standards by following procedure.
9. By only storing all business information on the relevant systems designated by the charity and by using only equipment approved by the Organisation.
10. The Information Asset Owner is responsible for ensuring that Information Asset Managers amend entries on the Information Asset Register to show the correct retention period from the schedule.
11. A policy review (at least annually) must review the provisions of the Retention Schedule within the ROPA and make any necessary amendments, documenting the reasons for change and managing affected records accordingly.
12. We must complete and retain archiving indexes providing the relevant information about paper records in storage, ensuring that the charity is aware of what information it holds at all times and when they can be reviewed.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Sue Rudgley - DPO sue@ete.org.uk

References

- Data Protection Act 1998 (to May 25th 2018)
- General Data Protection Regulations 2016 (from 25th May 2018)
- Article 8, The Human Rights Act 1998
- Freedom of Information Act 2000.
- Code of Practice on Records Management (under Section 46 of the FoIA)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.