Trust in Learning
Trust in Success

TRUST IN LEARNING (ACADEMIES)

RECORDS MANAGEMENT, RETENTION AND DISPOSAL POLICY

Trust in Learning
Trust in Success

Trust in Learning
Trust in Success

Date Created: March 2018
Effective From: May 2018
Dated Adopted by the Board: May 2018
Review Date: July 2022

Date	Page	Change	Purpose of Change
May 2018		New Policy	

1. **Policy Statement**

1.1. Records Management is the process by which the Trust and its associated schools manage all aspects of any type of 'record' whether internally or externally generated and in any format or media type, from their creation, throughout their lifecycle and to their eventual disposal.

1.2. This policy should be read and actioned in accordance with all the other Trust policies dealing with information governance.

2. **Definitions**

2.1. "*The Trust*" means Trust in Learning (Academies) and its associated schools.

2.2. *"Data"* means Personal Data and Special Category Personal Data.

2.3. *"Data Controller"* is the person who or the organisation which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation.

2.4. "*Data Subject*" means all living individuals about whom the Trust holds Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in respect of their Data and the information that the Trust holds about them.

2.5. *"Data Processor*" means any person who or organisation which processes Data on behalf of the Data Controller including contractors, and suppliers and any third party whose work involves accessing or otherwise using Data held by the Trust. Data Processors have a duty to protect the information they process for and on behalf of the Trust by following this and other Trust information governance policies at all times.

2.6. "*Data Protection Legislation*" means the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

2.7. "*Personal Data*" means any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

2.8. "*Processing*" means any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.

2.9."*Special Category Personal Data*" means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data

2.10."*Social Media"* means websites and applications that enable users to create and share content or to participate in social networking including Facebook, LinkedIn, Twitter, Google+, and all other social networking sites, internet postings and blogs. It applies to use of Social Media for Trust purposes as well as personal use that may affect the Trust in any way.

2.11. "*Subject Access Request*" ("SAR") means a request by an individual to the Trust pursuant to Article 15 of the GDPR.

2.12."data put beyond reasonable use" refers to some electronic data can't be physically deleted and in those circumstances the Trust will ensure that it is not in a live system and is not reachable by the data processor

3. **Relevant Data Protection Principles**

3.1.The data protection principles[1] which directly relate to the management, retention and disposal of Personal Data are that the Personal Data must be:

i. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Article 5(1)(c) of the GDPR)

ii. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Article 5(1)(d) of the GDPR

iii. be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (Article 5(1)(e) of the GDPR)

iv. be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5(1)(f) of the GDPR)

4. **Retention Periods**

4.1In line with Article 5(1)(e) of the GDPR as set out at 3.1 (iii) above the Trust will not retain Data in an identifiable form for any longer than necessary for the purpose for which it was obtained and in determining an appropriate retention period will take into account the following:

i. The current and future value of the Data.

ii. The costs, risks and liabilities associated with retaining the Data in an identifiable form.

iii. The ease or difficulty in ensuring the Data remains accurate and up-to-date.

iv. Any applicable statutory limitation periods.

v. Any relevant guidance documents.

[1] Contained in Schedule 1 to DPA.

4.2**Default Periods**

i. The default period is the minimum period for which the Trust will retain Data. At the conclusion of the default period, the Trust will review the Data being held and determine whether it can be destroyed in accordance with paragraph 6 below.

ii. The standard default period for retaining Data will be as set out in the Records Management Toolkit for Schools produced by the Records Management Society. This can be found at http://www.irms.org.uk/resources/information-guides/199-rm-toolkit-for-school

iii. The Trust will take into account the matters set out in paragraph 4.3 below in determining whether Data will be retained beyond the default period.

4.3**Exceptions to the Default Period**

i. In the majority of cases Data will be securely disposed of when it reaches the end of the retention period. When assessing whether Data should be retained beyond the retention period the Trust will consider whether:

(a)The Data is subject to a current request pursuant to the GDPR.

(b)The Trust is the subject of, or involved in ongoing legal action to which the Data is or may be relevant.

(c)The Data is or could be needed in connection with an ongoing investigation.

(d)The Data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, and the Trust has put in place appropriate technical and organisational measures.

(e)There are changes to the regulatory or statutory framework which require the Data to be retained for a longer period.

(f) The data subject has exercised their right to restrict the processing of the Data in accordance with Article 18 of the GDPR.

5. **Storage of Data**

Data will be stored in accordance with the Information Security Policy in place at the Trust from time to time.

6. **Disposal of Data**

6.1.When Data identified for disposal is destroyed, a register of the Data destroyed will be kept.

6.2.The destruction of Data is an irreversible act and must be clearly documented. All Data identified for disposal will be destroyed under confidential conditions by the Trust.

6.3.The Trust may sub-contract to another organisation its obligations to dispose of Data under confidential conditions.

6.4.Where the Trust sub-contracts its obligation to securely dispose of Data to a sub-contractor or other third party, the Trust will satisfy itself of the sub-contractor/third party's experience and competence to do so.

6.5.The decision for the destruction and disposal of Data must be made by nominated member of staff.

7. **Manual Records**
   Where Data is held in paper or other manual form, the default period for retaining Data has expired and none of the exceptions for retaining Data beyond the default period at set out at paragraph 4.3 (i) (a) to (e) is satisfied, the Trust will ensure the Data is shredded or otherwise confidentially disposed of by the Trust or by a person duly authorised by the Trust to confidentially destroy the Data.

8. **Electronic Records**
   8.1 Where Data is held in an electronic format the Trust will where feasible use its reasonable endeavours to:

   i. Put the Data beyond use so that the Data is no longer on a live electronic system and cannot be accessed by a Data Processor.

   ii. Ensure individuals within the Trust do not and will not attempt to access the Data or use the Data in any way in making a decision which will affect a Data Subject.

   iii. Surround the Data with such technical and security measures to ensure it is not accessible other than by a Data Processor.

   iv. Permanently delete the Data from the Trust's electronic systems when and where this becomes possible. The Trust will only engage Data Processors that are able to provide sufficient guarantees in relation to the secure disposal of Data.

   8.2 Where the steps set out at paragraph 8.1 (a) to (d) are complied with, the Trust considers the Data to be 'put beyond use' and this Data will not be used in order to respond to a Subject Access Request.

9. **Monitoring and Review**
   This policy will be reviewed by the nominated person responsible for data protection in the Trust every four years or earlier if required and may be subject to change.