Records Management Policy

Review Summary

Adopted:	***March 2018***
Review Cycle:	***Bi-annual***
Last Review:	***Sep 2020***
Next Review:	***May 2022***

1. Introduction

1.1 The Ted Wragg Multi Academy Trust (the trust) is committed to maintaining the confidentiality of information held about pupils, parents, staff and volunteers. In line with the requirements of the General Data Protection Regulation (GDPR), the Trust has a responsibility to ensure that all records are only kept for as long as is necessary to fulfil the purpose(s) for which they were originally intended.

1.2 This policy outlines how information will be processed, stored, accessed, monitored, retained and disposed of, to meet the Trust's statutory requirements to comply with the GDPR and other relevant statutory legislation.

1.3 The aim of this policy and the records retention schedule at Appendix A is to enable the Trust to comply with the commitments of the Data Protection Act 2018, General Data Protection Regulation (GDPR) and Act and Freedom of Information Act 2000 and integrates consideration of these and other compliance issues.

1.4 Records are defined as all documents and materials, regardless of format, which facilitate the activities carried out by the Trust. These records may be created, received and maintained in hard copy or electronically (including emails).

1.5 The Trust will manage records in line with the Records Retention Schedule, to ensure that it can meet Freedom of Information requests and respond to data subject access requests under the GDPR and other financial or legal requirements.

2. Objectives

2.1. Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

2.2. Records management helps to:

a. ensure that the Trust conducts itself in an efficient and accountable manner.
b. meet legislative and regulatory requirements.
c. support and document policy formation and decision-making.
d. facilitate the effective performance of activities and delivery of services throughout the Trust.
e. provide continuity in the event of a disaster.
f. protect the interests of the Trust in the event of litigation or otherwise.
g. establish and maintain the Trust's cultural identity and institutional memory.

3. Legal Framework and Related Policies

a. 3.1 This policy has due regard to the following legislation and guidance including, but not limited to, the following:

a. General Data Protection Regulation 2016 (became law in May 2018)
b. Data Protection Act 2018
c. Freedom of Information Act 2000
d. Limitation Act 1980

3.2 The following Trust policies also apply:

a. Data Protection Policy
b. Privacy Notices
c. Acceptable Use Policy (Staff)
d. Safeguarding and Child Protection Policy
e. HR Policies including Grievance, Disciplinary and Capability

4. Responsibilities

4.1. The Trust has a corporate responsibility to maintain its records and records management systems in accordance with legislation.

4.2. The Trust Director of Finance and Resources is responsible for providing guidance and advice on good records management practice. Such guidance is formulated within the context of existing Trust policies and guidelines, national legislation and sector-wide standards.

4.3. Each school within the Trust is individually responsible for the management of the records generated by its activities and to ensure all activities comply with this policy.

4.4. Individual members of staff should ensure that records, for which they are responsible, are maintained and disposed of in accordance with this policy.

5. Records Management Good Practice

5.1. When managing your records you must consider factors such as how your colleagues can access the files if necessary, how to ensure that records are kept for as long as necessary but not too long so as to be a burden on storage. Some general guidelines which may help to meet these and other aims are:

a. avoid duplication - create records only where necessary,
b. name files, electronic and paper, in a way that is meaningful to you and your colleagues,
c. avoid long, complicated numbering or coding that may be easy to misfile,
d. have a filing system that can be accessed by all that have a right to, while also balancing it with appropriate security arrangements, i.e. computer passwords, restricted access to shared folders and locked filing cabinets,
e. store material appropriately,
f. do not overfill boxes or cabinets,
g. sort files regularly,
h. dispose of records in a timely manner and use confidential waste collection or shredding facilities where available.

5.2 The length of time records should be kept can vary depending on the type of documentation and legal constraints, for more details on how long to keep specific records see the Trust's Disposal Schedule.

5.3 Records should be held in files - these may be paper based or held electronically in shared directories, databases or document management systems. The files should be organised in a structured way and have some indication as to their contents and relevance. Where there are confidentially issues, files may be held in a secure storage area, on a computer or email box but bear in mind that colleagues should be able to access them in your absence.

5.4 Exactly what records you keep on file will vary according to the work you do, however reasons for keeping records include but are not exhausted to:

a. There is a legal requirement to keep the information,

b. The information is needed to carry out the Trust's everyday business,

c. The information is for financial purposes,

d. Information explaining why and how a particular decision was made,

e. The information is needed if a decision is challenged, publicly accountable.

5.5 For most topics there should be one lead file. This will be the file of the person or department who has the lead on the topic concerned, for example, a committee clerk's set of minutes and papers. Other members of staff may also have a file on the same subject but they should keep this only for so long as is needed for their personal reference.

5.6 If you create a folder on a shared drive or on your personal drive, you should take responsibility for maintaining the contents of that folder. Do not allow out-of-date material to accumulate in it. If a document is not accessed in the course of eighteen months, it should probably be deleted from the drive unless it is the master file copy then it should be archived.

5.7 Documents and folders should have file titles which are easily understood by all members of staff. Do not name them after yourself, as this will be meaningless to others if you leave. Likewise, only use commonly understood abbreviations. The title should clearly indicate what the document is.

5.8 Do not use your computer hard drive (c:// drive) to store information as this drive is not backed up. Use your personal drive only for information which is confidential or personal or does not need to be shared within the Trust.

5.9 Shared drives should be used for current work to which your colleagues may need access. Password protection should be used where appropriate, whilst ensuring that material can be accessed in your absence by relevant colleagues. Folder permission restriction on the shared drive should be used to allow a restricted group of people to have appropriate levels of access.

5.10 Cloud storage or tools for sharing such as google drive or onefile must be set up with the same regard to permissions and access as for networked file systems.

6 Sending attachments

6.1 Avoid sending documents as attachments. Instead send a link or tell people where the document can be found. This ensures documents are less likely to get lost, or inappropriately shared, and everyone looks at the most up to date copy so there is no confusion over which version is the correct or latest one.

6.2 Egress Switch must be used when sending restricted documents outside the Trust network.

7 Confidential Records

7.1 These records should be labelled as 'Confidential' or 'Commercial in Confidence' and be clear as to who within the organisation should be able to access and use these records. It is also good practice for the record to hold an intended publication date, as few records remain confidential for their entire life-span.

7.2 N.B. Labelling a record 'Confidential' does not exempt the record from being admissible under the Freedom of Information Act 2000. Further information can be obtained from the Trust's Freedom of Information Policy

7.3 Information being supplied in confidence should be stamped, marked, or include a statement that it is confidential or being supplied in confidence, and be treated in a consistent confidential manner.

7.4 The following guidelines should be followed for confidential records:

a. Store confidential records in secure filing cabinets.

b. Cabinets should always be kept locked when not in use, not located in a public area, and access to the confidential records should be restricted only to those employees that require the information;

c. Confidential records should never be left in a public open area such as an in-tray or on a desk. The record should be returned to the cabinet when not in use;

d. Confidential records must be destroyed by confidential waste disposal or shredding only;

e. For electronic records, store confidential records in separate directories or files and restrict access to these directories or files;

f. Laptops that hold confidential information must be Trust owned and encrypted by IT Services; Confidential information should not be copied to non-Trust equipment;

8 E-Mails

8.1 E-mails may be disclosed in response to a freedom of information or data protection request and in legal cases. Electronic messages can be legally binding and the Trust may be held

liable for defamatory statements in e-mails. For these reasons, do not put anything in e-mails that you would not say in other forms of communication. If an e-mail contains important information or an important decision, it should be added to the relevant file/folder either electronically or a hard copy. An email can be saved electronically using 'File – Save as - File'.

8.2 The majority of emails produced are trivial; it is therefore, a drain on Trust resources to store them on our system and can cause a delay in responding to a subject request because of the additional time caused in searching through them. Under the Data Protection Act we should keep information about people for no longer than necessary; this includes e-mails to and from or about people. You should delete e-mails as soon as possible and should not allow a backlog to accumulate as this then becomes difficult to manage. Emails should also be deleted from your deleted items folder and/or recycle bin.

8.3 Because e-mail is a record you need to know that you can find it quickly and easily if you have to disclose it because of a Data Protection or Freedom of Information request.

8.4 E-mails need to be treated just like other records you deal with. You wouldn't leave paper mail piled up permanently in your in tray so you should treat your inbox in the same way. When you receive an e-mail act on it as soon as possible and then delete it. If it needs to be kept then file it.

8.5 Apart from the cost (environmental and financial) paper is easy to mislay. If the e-mail is needed to record official business procedure, note that paper printouts of e-mails don't hold the same legal weight as e-mails filed electronically.

9 Archive and Disposal

9.1 Documents should be archived in accordance with the Retention Schedule in Appendix A

9.2 You may wish to archive electronic files this should be done by creating an archive sub-folder on a Trust network drive. Within the archive sub-folder you can then create a folder named 'do not dispose' and numerous folders with the naming convention as the date of destruction. This will make it easier to dispose of the archived records when they reach their destruction date.

9.3 Before you begin to archive you will need to use items that are suitable for storing items long term such as archive cardboard boxes, paper files, plastic-ended treasury tags etc. as over time metal components may damage the files.

9.4 Documents and files need to be prepared prior to being put into the archive storage box. Files should be removed from lever arch files and placed into card wallets/files and all metal removed. The documentation should be reviewed to remove and destroy any paperwork that is not required to be stored, i.e. personal notes, duplicate items etc.

9.5 The first step to archiving your documents is to create an inventory. The best way to do this is by using a standard template detailing all the relevant information of the archive box contents.

10 Policy Circulation

10.1 This Policy will be published on the Trust's website and included in the Trust's Policy Monitoring Schedule.

10.2 This Policy will be circulated to every Member, Trustee/Director, Governor and Senior Employee by sending an email to the link on the Trust's website.

10.3 The Trustees are responsible for overseeing, reviewing and organising the revision of this Policy.

Adoption of the Policy

This Policy has been adopted by the Trustees of the Ted Wragg Multi Academy Trust**.**

Signed:

(Chair of Trust)

Date: 23.09.20