| | | |
|---|---|---|
| | **Name of School** | **Corbets Tey School** |
| | **Policy Review Date** | **18th November 2020** |
| | **Next Review Date** | **Spring 2022** |
| | **Reviewed by** | **Governor Name: Julie Lamb**<br>**Governor Signature:**  |

# Records Management Policy

**Equality Impact Assessment**
The school aims to design and implement services, policies and procedures that meet the diverse needs of our provision, population and workforce, ensuring that no-one is placed at an unreasonable or unfair advantage over others.

Where the school is referred to in this policy, the policy and the following procedures apply to all staff working for Corbets Tey School on all sites including staff at the Routes4Life provision.

**Introduction**
The School recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability.

This document provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

## 1. Scope of the policy

1.1. This policy applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

1.2. Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronic format.

## 2. Responsibilities

2.1 The governing board of a school has a statutory responsibility to maintain the school records and record keeping systems in accordance with the regulatory environment specific to the school. The person with overall responsibility for this policy is the Headteacher.

2.2 The person responsible for day-to-day operational management in the school will give guidance on good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 The school will manage and document its records disposal process in line with the Records Retention Schedule. This will help to ensure that it can meet Freedom of Information requests and respond to requests to access personal data under data protection legislation (subject access requests "SARS")

2.4 Individual staff and employees must ensure, with respect to records for which they are responsible, that they:

2.4.1 Manage the school's records consistently in accordance with the school's policies and procedures;

2.4.2 Properly document their actions and decisions;

2.4.3 Hold personal information securely;

2.4.4 Only share personal information appropriately and do not disclose it to any unauthorised third party;

2.4.5 Dispose of records securely in accordance with the school's Records Retention Schedule.

## 3. Relationship with existing policies

3.1 This policy has been drawn up within the context of:

- Freedom of Information Policy
- Data Protection Policy
- Information Management Toolkit for Schools 2019 - www.irms.org.uk

## 4. Storage of Records

4.1 The school's requirements for storage of records:

- Records must be able to be identified using a file reference or other unique identifier.
- Maintaining a system of identifying, classifying, storing and disposing of records.
- Coordination of secure access to sensitive records internally and from outside the organisation, balancing the requirements of confidentiality, data protection and public access
- Records must be stored in such a way that they are accessible and safeguarded against environmental damage.
- All files in current use must be stored appropriately.
- All student records must be kept securely at all times. Paper records should be kept in locked filing cabinets/storage areas and the contents should be secure within the file. Electronic records must have appropriate security.
- Access arrangements for student records should ensure that confidentiality is maintained whilst enabling information to be shared lawfully and appropriately, and to be accessible only by authorised personnel.
- Current staff records must be stored in a lockable cabinet or on the school network in a secure folder that is accessible only by persons authorised by the Headteacher or School Business Manager.
- Financial records to be stored appropriately by relevant staff.
- Management Information Systems – SIMS and FMS use is restricted to relevant staff members and password protected. Passwords must not be shared with any other person and must be changed termly.
- Closed records are either boxed up, clearly labelled and stored in the loft storage by the site manager or scanned and stored electronically on the school secure network. Files for archiving:
    - All records to be archived as per the Document Retention Schedule will be stored in appropriate boxes in the Loft Storage. Boxes will indicate contents and date of disposal.
    - Where applicable boxes will contain a contents list.
    - The Loft Storage is kept locked and access to these files is restricted to authorised personnel.

## 5. Document Retention Schedule

This school uses the Retention Schedule set out in the Retention Guidelines of the Information Management Toolkit for Schools 2019. The Retention Schedule is divided into 5 sections that cover the main categories of records held in school, statutory provisions (if applicable), the retention period and the action which should be taken once records reach the end of their administrative life or when they are of no further administrative or legal use.

Members of staff are expected to manage their current record keeping systems using the Retention Schedule and to take account of the different kinds of retention periods when they are creating new record keeping systems.

Members of staff should be aware that once a Freedom of Information request is received, or a legal hold imposed, then records disposal relating to the request or legal hold must be stopped.

Shortened versions of the Retention Schedule for general class-based and administration records are shown in Appendix 1 and 2.

**A full list of school based records for retention and retention periods can be found at:**
http://irms.org.uk/page/SchoolsToolkit

Records may be kept in hard copy and/or digitally. Please ask admin office staff for further guidance on scanning documents.

The school maintains an internal data map and audit record list of all personal data that we hold of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, how and why we are sharing the data and who with, retention periods and how we are keeping the data secure.

## 6. Safe disposal of records which have reached the end of their administrative life

6.1 The fifth data protection principle states that “Personal data must be kept for no longer than is necessary for the purpose for which it is processed”. Therefore, all records, in all formats, should be subject to an applicable retention period, as defined by business, statutory, regulatory, legal or historical requirements.

6.2 All records in all formats must be assigned a retention period and disposal date, either upon creation or when they cease to be in active use, in accordance with the Retention Schedule or policy. A system should be implemented to routinely identify records as soon as they reach their disposal date. This may form part of an electronic record-keeping system or a manual system.

6.3 Disposal must be carried out in a timely manner to:

- 6.3.1 Ensure compliance with business and legal retention requirements
- 6.3.2 Improve the efficiency of the record keeping system
- 6.3.3 Free up storage space
- 6.3.4 Reduce associated storage and management costs

6.4 Destruction must include all backup and duplicate copies, in all formats. This is especially vital for personal information which may be kept in various hybrid record keeping systems.

6.5 The disposal method must be applicable to the content and format of the information. Paper and electronic records should be disposed of separately, i.e. floppy disks, CDs, DVDs, tapes, USBs etc., should not be put into confidential waste containers containing paper as they require different disposal methods.

6.6 Destruction must be undertaken in a way that preserves the confidentiality of the information and which makes it permanently unreadable or unable to be reconstructed or reinstated. Special care should be taken when destroying personal, sensitive or commercial information and confidentiality should be paramount at all stages of the process.

## 7. Destruction of Records by Type

7.1 Paper Records

All hard copies of official records and those containing personal data must be destroyed using confidential methods, rather than being placed in general waste bins or skips, which could result in a data breach. The school uses a specialist company for the supply of confidential waste paper bins. Alternatively, records can be destroyed using a cross cut shredder and disposed of with paper waste.

7.2 Electronic and Other Media Records

Deletion of electronic records should be a managed and auditable process in the same manner as paper records. Records should be routinely identified for deletion and should be authorised by the relevant senior officer. Before deletion, it must be determined that all legal and business requirements have expired, and that there is no related litigation or investigation. Records must be securely deleted in accordance with the school's security policy. Processes must be in place to ensure that all backups and copies are included in the deletion process.

## 8. Documenting of all Archiving, Destruction, Deletion and Digitisation of Records

To satisfy audit, accountability, legal and business needs, it is vital to keep a record of all archiving, destruction, deletion and digitisation. The Freedom of Information Act 2000 requires schools to maintain a list of records which have been destroyed and a record of who authorised their destruction.

The Freedom of Information Act 2000 states that, as a minimum, the school should be able to provide evidence that the destruction of records took place as part of a routine records management process. Schools must assess whether they are creating another piece of Personal Identifiable Information (PII) by maintaining a record of evidence, particularly if they are listing the names of the people whose records have been deleted.

A record should be retained of:

- File reference (or another unique identifier)
- File title (or brief description)
- Number of files or volumes
- Date range
- Reference to the applicable retention period
- The name of the authorising officer
- Date approved for disposal
- Date destroyed or deleted from system
- Method of disposal
- Place of disposal (whether on-site or off-site by a contractor)
- Person(s) who undertook destruction

**A sample template for schedule of records destroyed can be found at:**
http://irms.org.uk/page/SchoolsToolkit

**Appendix 1 – Retention Schedule for general class based records**

If the item you are looking up is not shown below please view the full list in the IRMS Toolkit for Schools 2019 shown at http://irms.org.uk/page/SchoolsToolkit

| Record description | Retention period | Action at end of retention period |
|---|---|---|
| Schemes of Work | Current year + 1 year | SECURE DISPOSAL |
| Students' Work | Where possible, students' work should be returned to the student at the end of the academic year. | SECURE DISPOSAL |
| Record of homework set | Current year + 1 year | SECURE DISPOSAL |
| Day Books (Home School Diary) | Current year + 2 years then review | SECURE DISPOSAL |
| Parental/carer consent forms for school trips where there has been no major incident | Conclusion of the trip | SECURE DISPOSAL |
| Parental/carer permission slips for school trips – where there has been a major incident | DOB of the student involved in the incident + 25 years<br><br>The permission slips for all the students on the trip need to be retained to show that the rules had been followed for all students | SECURE DISPOSAL |
| Special Educational Needs files, reviews and Education, Health and Care Plans, including advice and information provided to parents/carers regarding educational needs and accessibility strategy | Date of birth of the student + 31 years<br>[Education, Health and Care Plan is valid until the individual reaches the age of 25 years – the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act] | NOTE: This retention period is the minimum retention period that any student file should be kept. Some authorities choose to keep SEN files for a longer period of time to defend themselves in a "failure to provide a sufficient education" case. There is an element of business risk analysis involved in any decision to keep the records longer than the minimum retention period and this should be documented. |
| Reports for outside agencies - where the report has been included on the case file created by the outside agency | Whilst student is attending school and then destroy | SECURE DISPOSAL |

**Appendix 2 – Retention Schedule for general administration based records**

If the item you are looking up is not shown below please view the full list in the IRMS Toolkit for Schools 2019 shown at http://irms.org.uk/page/SchoolsToolkit

| Record description | Retention period | Action at end of retention period |
|---|---|---|
| Attendance Registers (students) | Every entry in the attendance register must be preserved for a period of 3 years after the date on which the entry was made. | SECURE DISPOSAL |
| Correspondence relating to any absence (authorised or unauthorised) (students) | Current academic year + 2 years | SECURE DISPOSAL |
| Newsletters and other items with a short operational use | Current academic year + 1 year | STANDARD DISPOSAL |
| Visitor management systems (including electronic systems, visitors books and signing-in sheets) | Last entry in the visitor book + 6 years (in case of claims by parents, carers or students about various actions). | SECURE DISPOSAL |
| All records leading up to the appointment of a member of staff/governor – unsuccessful candidates | Date of appointment of successful candidate + 6 months | SECURE DISPOSAL |
| Pre-employment vetting information – DBS Checks – successful candidates | Application forms, references and other documents – for the duration of the employee's employment + 6 years.<br><br>The school does not keep copies of DBS certificates but keeps a record of the reference number and the date of issue. | SECURE DISPOSAL |
| Forms of proof of identity collected as part of the process of checking "portable" enhanced DBS disclosure | Where possible this process should be carried out using the on-line system. If it is necessary to take a copy of documentation then it should be retained on the staff personal file. | SECURE DISPOSAL |
| Pre-employment vetting information – Evidence proving the right to work in the United Kingdom – successful candidates | Where possible these documents should be added to the staff personnel file. If they are kept separately then the Home Office requires that the documents are kept for termination of employment + not less than 2 years | SECURE DISPOSAL |