Ravensbury Community School
RECORDS MANAGEMENT POLICY

1. 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.

2. Scope of the Policy

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

2.2 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-see appendix) to provide evidence of its transactions or activities. These records may be created or received, and then stored, in hard copy or electronically.

2.3 A small percentage of the school's records may be selected for permanent preservation as part of the institution's archives and for historical research.

3. Responsibilities

3.1 The school has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Headteacher.

3.2 The person responsible for records management in the school will give guidance about 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.

3.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the school's records management guidelines.

4. Relationship with other policies

This policy has been drawn up within the context of the Freedom of Information policy, Data Protection policy and with other legislation or regulations (including audit, equal opportunities and ethics) affecting the school.

5. Recording Systems

Information created by the school must be managed against the same standards regardless of the media in which it is stored.

Maintenance of Record Keeping Systems

- It is important that filing information is properly resourced and is carried out on a regular basis. It is also important that the files are weeded of extraneous
- information where appropriate on a regular basis. Removing information from a file once a subject access request has been made will be a criminal offence (unless it is part of normal processing).

- Applying retention periods is straightforward provided files are closed on a regular basis.
- Once a file has been closed, it should be moved out of the current filing system and archived until it has reached the end of the retention period (see appendix).
- Information security is very important especially when dealing with personal information or sensitive information. There are a number of basic rules which the school will follow:

a. All personal information should be kept in lockable filing cabinets which are kept locked when the room is unattended;
b. Personal information held on computer systems should be adequately password protected. Information should never be left up on a screen if the computer is unattended;
c. Files containing personal or sensitive information should not be left out on desks over night;
d. Where possible sensitive personal information should not be sent by e-mail;
e. If files need to be taken off the premises they should be secured in the boot of a car in lockable containers and returned to the author on return;
f. Teachers may carry data on memory sticks, provided by the school, or other removable data carriers in order to access their files both at home and at school. Any data carried in this way must be encrypted using appropriate encryption software;
g. All computer information should be backed up regularly and the back-up should be stored off site.
h. Information contained in email, fax should be filed into the appropriate electronic or manual filing system once it has been dealt with.

6. Managing Pupil Records

Recording information

A pupil or their nominated representative (for pupils aged 12 and under) have the legal right to see their file at any point during their education and even until the record is de stroyed (when the pupil is 25 years of age or 35 years from date of closure for pupils with special educational needs). This is their right of subject access under the GDPR 2018. It is important to remember that all information should be accurately recorded, objective in nature and expressed in a professional manner. The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career. It is essential that files, which contain personal information, are managed within the data protection guidelines.

The following information should appear on the school system:

- Surname
- Forename
- Preferred name
- DOB
- Unique Pupil Number

- The name of the pupil's doctor
- Emergency contact details
- Gender
- Position in family
- Ethnic origin (although this is "sensitive" data under the GDPR 2018, the Department for Education require statistics about ethnicity])
- Home Language (if other than English)
- Religion
- Names of adults who hold parental responsibility with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Information about previous setting: Name of the school, admission number and the date of admission and the date of leaving.
- Any allergies or other medical conditions that it is important to be aware of.
- Special Educational Needs Yes/No (This is to enable the files of children with special educational needs to be easily identified for longer retention).

Additional information will also be recorded and included in the pupil record

- Attendance
- Any information relating to exclusions (fixed or permanent)
- Absence notes and/or reasons for absence
- Any relevant medical information including health care plans (should be stored in the file in a sealed envelope clearly marked as such)
- Admission form (application form)
- Privacy Notice (if these are issued annually only the most recent need be on the file)
- Photography Consents
- Annual Written Report to Parents including a record of National Curriculum attainment.
- Any information relating to a major incident involving the child (either an accident or other incident)
- Accident forms (these should be stored separately and retained on the school premises until their statutory retention period is reached. A copy will be attached to the pupil file in the event of a major incident.
- Any correspondence with parents or outside agencies relating to major incidents.
- Child protection reports/disclosures (will be sent separately and clearly marked as such. It will be signed for upon receipt)

A Data Collection form will be completed by parents on registration and at least annually. A copy of the original will be saved electronically. The original will be disposed of.

7. Storage of pupil records

All pupil records will be stored electronically with appropriate security and only be accessible for those who are authorised to see it. Paper records should be kept in lockable storage

8. Transferring the pupil record to High school

A CTF (Common Transfer Form) and all electronic documents which relate to the pupil file will be sent to the receiving high school at the end of Y6. The pupil record should not be weeded before transfer to the high school unless any records with a short retention period have been placed in the file. It is important to remember that the information which may seem unnecessary to the person weeding the file may be a vital piece of information required at a later stage. Files should not be sent by post unless absolutely necessary. If files are sent by post, they should be sent by registered post with an accompanying list of the files. The High School should sign to say they have received the files of children attending their school. Where appropriate, records can be delivered by hand with signed confirmation for tracking and auditing purposes. The primary school will hold an electronic copy of the pupil file for 12 months after the pupil has left. Custody of and responsibility for the records passes to the school the pupil transfers to.

9. The Safe Disposal of Information Using the Retention Schedule

Files should be disposed of in line with the attached retention schedule (see appendix).

- This is a process which should be undertaken on an annual basis during the month of September.
- Paper records containing personal information should be disposed of in the 'Shred-it' sensitive document bins.
- CD's/DVD's/Floppy disks should be cut into pieces.
- Audio/Video tapes and fax rolls should be dismantled and shredded.
- Computer hard drives should be removed from the device and disposed of securely.
- Electronic data should be archived on electronic media and 'deleted' appropriately at the end of the retention period.

10. Managing E-mail

These guidelines are intended to help school staff to manage their e-mail in the most effective way, and must be used in conjunction with the school's ICT acceptable user policy

E-mail is not always a secure medium to send confidential information. Confidential or sensitive information should only be sent by a secure encrypted e-mail system. Personal information (such as a pupil's name) should never be put in the subject line of an e-mail.

All school e-mail is disclosable under Freedom of Information (SAR) and Data Protection legislation. Anything you write in an email could potentially be made public. E-mail is not necessarily deleted immediately they can remain in a system for a period of time after you have deleted them. Be mindful that although your copy of an e-mail may have been deleted, the recipients may not and therefore there will still be copies in existence. These copies could be disclosable under the Freedom of Information Act 2000 or under GDPR 2018.

Agreements entered into by e-mail can form a contract. Individual members of staff should not enter into agreements either with other members of staff internally or with external contractors unless they are authorised to do so. All attachments in e-mail should be saved into any appropriate electronic filing system or printed out and placed in paper files.

Any employer has a right to monitor the use of e-mail provided it has informed members of staff that it may do so.

Creating and sending e-mail

Never send on chain e-mails. When sending emails containing personal or sensitive data always respond to an authorised, approved address. All emails that are used for official business must be sent from an official business domain address. Use a consistent method of defining a subject line; do not use any personal information which could identity a child.

- Do not use text language or informal language in school e-mails.
- Always sign off with a name (and contact details).

Disclaimers

Adding a disclaimer to an e-mail mitigates risk, such as sending information to the wrong recipient, or helps to clarify the school's position in relation to the information being e-mailed. Typically, they cover the fact that information may be confidential, the intention of being solely used by the intended recipient, and any views or opinions of the sender are not necessarily those of the school.

Managing received e-mails

Using an out of office message

During school holidays it is appropriate to set your work email to Out of Office AutoReply this will tell the recipient when they might expect a reply.

Filing e-mail

Where the main purpose of the e-mail is to transfer documents, then the documents should be saved into the appropriate place in an electronic filing system or printed out and added to a paper file. The e-mail can then be deleted.

Emails should be kept electronically for two years.

11. Digital Information

In order to mitigate against the loss of electronic information a school:

a. Operates an effective back-up system

b. Control the way data is stored within the school

Personal information must not be stored on the hard drive of any laptop or PC unless the device is running encryption software. Staff are advised not to hold personal information about students or other staff on mobile storage devices including but not limited to memory sticks, phones, iPads, portable hard drives or even on CD.

c. Maintain strict control of passwords

Ensure that the data is subject to a robust password protection regime, ideally with users changing their passwords every 30 days. Password sharing is strongly discouraged. Staff should always lock their PCs when they are away from the desk to prevent unauthorised use.

d. Manage the location of server equipment

The server environment is managed to prevent access by unauthorised people.

e. Ensure that business continuity plans are tested

12. Hard Copy Information and Records

Records which are not stored on the school's servers are at greater risk of damage by fire and flood as well as risk of loss and of unauthorised access.

a. Fire and flood

In order to limit the amount of damage which a fire or flood can do to paper records, all vital information should be stored in lockable filing cabinets, drawers or cupboards.

13. Unauthorised access, theft or loss

Staff should be encouraged not to take personal data on staff or students out of the school, and where these records are held within the school they should be in lockable cabinets with restricted access. All archive or records storage areas should be lockable and have restricted ac cess. Where paper files are checked out from a central system a log the location of the file is kept and the borrower, creating an audit trail.

14. Clear Desk Policy

The school operates a clear desk policy to avoid unauthorised access to physical records which contain sensitive or personal information and will protect physical records from fire and/or flood damage. A clear desk policy involves the removal of the physical records which have been identified to a cupboard or drawer (lockable where appropriate). It does not mean that the whole desk has to be cleared.

15. Disclosure

Staff are aware of the importance of ensuring that personal information is only disclosed to people who are entitled to receive it. No information is shared with a third party with consent.

16. Major Data Loss/Information Security Breach

A clear process is in place if there is a major data loss or information security breach. This will involve the schools DPO (Global Policing) liaising with the Information Commissioners Office if an information security breach needs to be reported.

17. Monitoring and Review

This policy has been reviewed and approved by the head teacher and governors. The Records Management Policy will be reviewed and updated as necessary every 3 years.

Retention Guidelines

Under the Freedom of Information Act 2000, school maintains a retention schedule listing the record series which the school creates in the course of its business. The retention schedule lays down the length of time which the record need to be retained and the action which should be taken when it is of no further administrative use. The retention schedule lays down the basis
for normal processing under both GDPR 2018 and the Freedom of Information Act 2000.
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. The retention schedule refers to record series regardless of the media in which they are stored.