

# Records Management Policy

**Our vision:** Templars, a place where everyone belongs. A place where everyone is proud to belong. A school where everyone is welcomed, feels safe and strives to achieve their full potential.

**Our mission:** Every child, Every day, Every chance.

**Our values:** Care, Respect and Honesty.

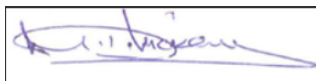
## Document Control

| Item            | Detail                                        |
|-----------------|-----------------------------------------------|
| Policy Author   | Helen Benarous/Headteacher                    |
| Policy Owner    | Headteacher                                   |
| Approval        | Governing Board                               |
| Date Ratified   | Autumn 2026                                   |
| Review Cycle    | Bi-Annually                                   |
| Next Review Due | Autumn 2028 (or sooner if statutory guidance) |

## Signatures

| Role        | Name           | Signature                                                                           | Date    |
|-------------|----------------|-------------------------------------------------------------------------------------|---------|
| Headteacher | Helen Benarous |  | 16.8.26 |

Chair of Governors Martin Vickery



## Distribution

- Available on the school website
- Available from the school office on request
- Shared with staff on Sharepoint



## 1. Purpose

Templars Primary School creates and holds records in order to educate and safeguard pupils, employ and support staff, manage the school effectively, meet its statutory responsibilities and provide evidence of its decisions and actions.

Good records management supports:

- effective teaching, safeguarding and pastoral care;
- continuity when pupils or staff move;
- sound decision-making and accountability;
- efficient school administration;
- compliance with legal, regulatory and financial requirements;
- protection of the rights and interests of pupils, families, staff and the school;
- appropriate responses to information rights requests, complaints, investigations and legal proceedings; and
- preservation of records of enduring historical value where appropriate.

This policy establishes the principles by which records are created, managed, stored, accessed, retained, transferred and securely disposed of.

It applies to records in **all formats and locations**, including paper and electronic records, emails, management information systems, safeguarding systems, cloud platforms, SharePoint, photographs, video, CCTV, audio recordings and other digital systems.

## 2. Scope

This policy applies to all records created, received, maintained or held by or on behalf of Templars Primary School in connection with its functions.

This includes records relating to:

- pupils and former pupils;
- parents and carers;
- safeguarding and child protection;
- SEND and additional needs;
- attendance;
- behaviour;
- teaching, assessment and curriculum;
- staff, recruitment and employment;
- governors and governance;
- finance and procurement;
- health and safety;
- premises and assets;
- complaints;

- 
- correspondence and communications;
  - contracts and suppliers; and
  - the management and administration of the school.

The policy applies to all employees, governors, volunteers and others who create, receive or manage school records as part of their role.

Records created while carrying out school business remain school records regardless of the device, system or location in which they were created.

### **3. Legal and Regulatory Framework**

The school manages records in accordance with relevant legislation and statutory requirements, including, where applicable:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- Education Act 1996;
- Children Act 1989 and Children Act 2004;
- Equality Act 2010;
- Limitation Act 1980;
- relevant financial, employment and health and safety legislation; and
- statutory safeguarding requirements, including **Keeping Children Safe in Education**.

The school also has regard to current guidance issued by the Department for Education, Information Commissioner's Office and other relevant regulatory bodies.

The Data (Use and Access) Act 2025 does not replace UK GDPR or the Data Protection Act 2018 but amends and builds upon the existing framework.

### **4. Records Management Principles**

The school will ensure, as far as reasonably practicable, that records are:

**Accurate** – records should provide a reliable account of the information, action, decision or event they document.

**Adequate and relevant** – sufficient information should be recorded for the purpose for which the record is required, without collecting or retaining unnecessary information.

**Clear** – records should be written in a way that can be understood by an appropriate person who may need to use them in future.

**Authentic** – it should be possible to establish what a record relates to, who created it and, where relevant, when it was created or amended.

**Secure** – records must be protected against unauthorised access, alteration, loss, destruction or disclosure.

**Accessible** – authorised people should be able to locate and retrieve information when it is legitimately required.



**Retained appropriately** – records must be kept for as long as they are required, but not indefinitely without justification.

**Disposed of securely** – records that have reached the end of their retention period and are no longer required must be securely destroyed or anonymised unless there is a legitimate reason for continued retention.

The ICO's storage-limitation principle requires organisations to be able to justify how long personal information is retained and to review and erase or anonymise information when it is no longer required.

## **5. Roles and Responsibilities**

### **Governing Board**

The Governing Board is responsible for:

- ensuring appropriate records-management and data-protection arrangements are in place;
- approving this policy;
- providing appropriate oversight; and
- ensuring the school has access to appropriate Data Protection Officer advice.

### **Headteacher**

The Headteacher has overall operational responsibility for ensuring that effective records-management arrangements are implemented across the school.

This includes ensuring that:

- staff understand their responsibilities;
- appropriate systems and procedures are in place;
- records are stored and handled securely;
- the Record Retention Schedule is implemented;
- information incidents are appropriately managed; and
- appropriate advice is sought where required.

### **Data Protection Officer**

The Data Protection Officer (DPO) provides independent advice and oversight in relation to the school's compliance with data-protection legislation.

The DPO may advise on:

- retention and disposal;
- information rights requests;
- data breaches;
- data sharing;
- privacy risks;
- records containing personal information; and
- other data-protection matters.

### **Designated Safeguarding Lead**

The Designated Safeguarding Lead (DSL) is responsible for ensuring that safeguarding and child-protection records are created, maintained, accessed, transferred and retained in accordance with current statutory safeguarding requirements and school procedures.

### **School Business Manager and Administrative Staff**

Staff with administrative, finance, HR or records-management responsibilities will ensure that records within their areas are managed in accordance with this policy and the Record Retention Schedule.

### **All Staff**

Everyone who handles personal data in school has responsibility for protecting it. Current DfE guidance explicitly applies that responsibility to all staff.

Staff must:

- create accurate and appropriate records;
- use school-approved systems;
- store information securely;
- only access information they are authorised to access;
- not remove, alter or destroy records without authority;
- follow the Record Retention Schedule;
- report loss, unauthorised disclosure or other information incidents promptly; and
- seek advice where they are uncertain about how a record should be handled.

### **6. Creating and Maintaining Records**

Records should be created where they are necessary to provide evidence of school business, decisions, actions, events or responsibilities.

Records should be:

- factual and accurate;
- created promptly;
- dated where appropriate;
- attributable to the person creating them;
- written professionally;
- sufficiently detailed to enable the matter to be understood later; and
- stored in the appropriate school system or location.

Staff should distinguish clearly between fact, professional judgement, opinion and information reported by another person.

Records should not contain unnecessary, excessive, speculative or inappropriate personal comments.

Where an error is identified, the record should be corrected in a way that preserves an appropriate audit trail where required. Records should not be altered or deleted simply because their content later becomes inconvenient or disputed.

Staff should work on the basis that records containing personal information may potentially be disclosed to the person concerned through information-rights legislation, subject to any applicable exemptions.

### **7. Pupil and Educational Records**

The school will maintain appropriate records for each pupil.

Records may include, where relevant:

- admission and identification information;

- 
- attendance;
  - assessment and attainment;
  - curriculum and educational information;
  - SEND and additional-needs information;
  - behaviour and pastoral information;
  - medical information required by the school;
  - communications with parents/carers;
  - reports;
  - information received from previous education settings;
  - information about support and interventions; and
  - other information necessary to educate, support or safeguard the pupil.

Pupil records must be managed securely and access restricted to those with a legitimate reason to view them.

Information should be stored within the appropriate school system rather than unnecessarily duplicated across personal folders, emails or local devices.

When a pupil leaves the school, relevant records will be transferred and/or retained in accordance with statutory requirements and the school's Record Retention Schedule.

The school will maintain sufficient evidence of significant record transfers where appropriate.

### **8. Safeguarding and Child Protection Records**

Safeguarding records require particularly careful management because of their sensitivity and importance to children's welfare.

Safeguarding and child-protection records must:

- be accurate, clear and appropriately detailed;
- distinguish fact from opinion;
- identify the concern or allegation;
- record actions taken;
- record decisions reached and the rationale for those decisions where appropriate;
- record relevant outcomes;
- be stored securely;
- be accessible only to those who require access for legitimate safeguarding purposes; and
- be retained and transferred in accordance with current statutory safeguarding requirements.

Safeguarding records must be maintained separately from the ordinary pupil educational record, whether held physically or electronically.

#### **Transfer to another school or college**

When a pupil transfers to another school or college, the DSL will ensure that the child-protection file is transferred:

- **separately from the main pupil file;**
- securely;

- as soon as practicable in accordance with current safeguarding requirements; and
- with confirmation of receipt obtained and retained where required.

The receiving DSL should be informed of information necessary to enable appropriate support to be put in place.

The school will not routinely create or retain unnecessary duplicate copies of transferred safeguarding case files. Any records retained following transfer will be those required by the Record Retention Schedule or necessary to evidence the transfer or meet another legitimate requirement.

Current DfE retention guidance states that child-protection files should be passed to a child's new school separately from the main pupil file.

### **Allegations relating to staff**

Records relating to allegations against staff will be managed in accordance with current **Keeping Children Safe in Education**, the school's safeguarding procedures and the Record Retention Schedule.

KCSIE 2026 distinguishes between allegations found to be malicious or false and other outcomes. Details of allegations found following investigation to be malicious or false should normally be removed from personnel records unless the individual consents to their retention. Records of other allegations require an appropriate summary, outcome and record of actions and decisions.

Low-level concerns will be managed in accordance with KCSIE and the school's Low-Level Concerns procedures.

### **9. SEND and Additional-Needs Records**

Records relating to SEND and additional needs must be accurate, relevant and proportionate.

The school will distinguish between:

- statutory or significant records requiring longer-term retention; and
- routine working documents or duplicated information that does not require equivalent retention.

Relevant records may include:

- Education, Health and Care Plan documentation;
- statutory assessment information;
- professional reports;
- records of significant provision and support;
- review documentation;
- correspondence with external agencies; and
- other information necessary to demonstrate how the school has identified and met a pupil's needs.

SEND information must not be retained indefinitely simply because it relates to SEND.

Records will be retained in accordance with their purpose and the Record Retention Schedule.

### **10. Storage and Security**



Records must be stored in a manner appropriate to their sensitivity and importance.

### **Paper records**

Confidential paper records should:

- be stored securely;
- be protected from unauthorised access;
- not be left unattended in public or insecure areas;
- only be removed from school where authorised and necessary; and
- be transported securely where removal is necessary.

### **Electronic records**

Electronic records must be stored using school-approved systems and must be protected through appropriate technical and organisational security measures.

Staff must follow the school's requirements relating to:

- passwords and authentication;
- access permissions;
- devices;
- remote working;
- cloud services;
- email;
- cyber security;
- removable media; and
- reporting security incidents.

Personal accounts, personal cloud-storage services and unauthorised devices or applications must not be used to store school records.

Detailed requirements are set out in the school's **Accountable Use of ICT, Online Services and Digital Technology Policy**.

## **11. Email, Messaging and Digital Communications**

Email and other electronic communications may constitute school records.

Where a communication provides significant evidence of:

- a decision;
- an agreement;
- an action;
- a safeguarding matter;
- a complaint;
- professional advice;
- a contractual matter; or
- another significant school activity,

it should be retained in the appropriate school record or system where necessary.

Staff should not use their email inbox as the sole long-term repository for important school records.

Routine emails and messages with no continuing business, legal, safeguarding or evidential value do not need to be retained indefinitely.



The same retention principles apply to electronic information regardless of whether it is held in email, SharePoint, an MIS, CPOMS, another cloud service or an archived system.

## **12. Information Mapping and Records of Processing**

The school will maintain appropriate documentation of the personal information it processes.

This should enable the school to understand, where appropriate:

- what information it holds;
- why it holds it;
- whose information it is;
- where it is stored;
- who has access to it;
- who it is shared with;
- the lawful basis for processing;
- how long it should be retained; and
- how it will ultimately be disposed of.

The school's information asset register, record of processing activities and Record Retention Schedule may be used together to provide this oversight.

## **13. Access to Records and Information Rights**

Access to school records is restricted according to role and legitimate need.

Employees must not access records merely because the system allows them to do so.

Requests for access to information may arise under:

- UK GDPR/Data Protection Act 2018;
- Freedom of Information Act 2000;
- Environmental Information Regulations 2004;
- education legislation; or
- other legal processes.

Such requests must be referred promptly to the appropriate person and handled in accordance with the school's relevant procedures.

Good record keeping and appropriate retention arrangements make it easier for schools to respond properly to subject access requests.

Staff must not delete, alter or destroy information because a request for access, complaint, investigation, legal claim or other relevant process has been made or is reasonably anticipated.

## **14. Sharing Records**

Information will only be shared where there is a lawful and legitimate reason to do so.

Before sharing information, staff should consider:

- whether sharing is necessary;
- whether the recipient is appropriate;
- what information is actually required;
- whether the information can be shared securely; and
- whether any particular safeguarding or confidentiality requirements apply.



Data protection law does **not** prevent appropriate information sharing for safeguarding purposes.

Where there is uncertainty, advice should be sought from the DSL, DPO or another appropriate senior leader according to the nature of the information.

### **15. Transfer of Records**

Records transferred within or outside the school must be handled securely.

The method of transfer should reflect the sensitivity of the information.

Where appropriate, the school will:

- verify the intended recipient;
- use an approved secure transfer method;
- maintain appropriate records of transfer;
- obtain confirmation of receipt; and
- avoid retaining unnecessary duplicate copies.

Where records are transferred to another organisation, responsibility for retention should be clear.

Particular requirements for safeguarding records are set out in Section 8.

### **16. Record Retention Schedule**

The school's **Record Retention Schedule** forms part of its records-management arrangements and must be followed by all staff.

The schedule identifies:

- categories of records;
- standard retention periods;
- the event from which the retention period runs where appropriate; and
- the action to be taken at the end of the retention period.

Retention periods may be based on:

- statutory requirements;
- safeguarding requirements;
- regulatory guidance;
- limitation periods;
- financial or audit requirements;
- contractual requirements;
- operational need; and
- recognised records-management practice.

The UK GDPR does not establish one universal period for retaining personal data. The school must be able to justify its retention periods according to the purpose for which information is held.

#### **Exceptions to standard retention periods**

A record must **not** be destroyed simply because its standard retention period has expired where it remains relevant to:

- an ongoing safeguarding matter;
- litigation or a potential legal claim;

- 
- a complaint;
  - an investigation;
  - an insurance matter;
  - an audit;
  - an information-rights request;
  - a police or regulatory matter; or
  - another legitimate reason requiring continued retention.

In these circumstances, destruction should be suspended until it is confirmed that the record may lawfully be disposed of.

Where there is uncertainty about the appropriate retention period, **the record must not be destroyed until advice has been obtained from the Data Protection Officer and, where relevant, the Designated Safeguarding Lead or other appropriate professional adviser.**

### **17. Reviewing and Weeding Records**

Records should be reviewed periodically to ensure that information is not retained unnecessarily.

The school will make appropriate arrangements for regular review and disposal of records that have reached the end of their retention period.

Departments and record owners should not accumulate records indefinitely.

Review may include:

- deleting duplicate copies;
- removing superseded working documents;
- deleting routine correspondence that no longer has value;
- identifying records that have reached their disposal date;
- anonymising information where identification is no longer required; and
- identifying records that should be retained for longer because of a legitimate reason.

ICO guidance specifically recommends periodic weeding to prevent information becoming excessive, inaccurate or unnecessarily retained.

### **18. Archives, Backups and Deleted Accounts**

Moving information from an active system into an **archive does not itself satisfy the requirement to delete information** when its retention period expires.

Retention and disposal requirements apply to electronic and archived records as well as paper records.

The school will work with relevant system providers and IT support to ensure that, as far as reasonably practicable:

- archived information is subject to appropriate retention arrangements;
- records associated with former users are appropriately reviewed;
- information is not retained indefinitely merely because a system permits it;
- backup arrangements are appropriate and secure; and
- deleted information is dealt with in accordance with system capabilities, contractual arrangements and data-protection requirements.



Backups are primarily maintained for system recovery and business continuity and should not routinely be used as permanent archives.

### **19. Secure Disposal and Destruction**

Records that have reached the end of their retention period and are no longer required will be securely disposed of.

#### **Paper records**

Confidential paper records must be destroyed through an approved secure method, such as confidential-waste destruction or cross-cut shredding as appropriate.

They must not be placed in ordinary waste or recycling where personal, confidential or sensitive information could be reconstructed or accessed.

#### **Electronic records**

Electronic records must be securely deleted using an appropriate method.

Deleting a shortcut, moving a file to a recycle bin or removing information from an individual's view may not constitute secure deletion.

Where devices or storage media are being reused, transferred or disposed of, school information must be securely erased in accordance with the school's ICT and asset-disposal arrangements.

Where destruction is carried out by an external provider, appropriate assurances and contractual arrangements must be in place.

Records of destruction should be retained where this is appropriate because of the nature or sensitivity of the records concerned.

### **20. Records of Historical Value**

Some records may have enduring historical or archival value.

Where the school considers that a record should be retained permanently for legitimate historical or archival purposes, this should be identified within its records-management arrangements.

Any continued retention of personal information for archiving purposes must comply with applicable data-protection requirements and appropriate safeguards.

Records must not simply be kept permanently because they are interesting or *might* be useful one day.

### **21. Loss, Damage or Unauthorised Disclosure of Records**

Any actual or suspected:

- loss of records;
- unauthorised access;
- accidental disclosure;
- inappropriate alteration;
- destruction;
- theft;
- cyber incident affecting records; or
- other personal-data breach

must be reported **immediately** through the school's agreed reporting procedures.



Staff must not attempt to conceal an information incident.

The Headteacher, DPO, DSL and/or IT support will be involved according to the nature of the incident.

Where required, the school will assess whether the incident must be reported to the Information Commissioner's Office, affected individuals, police, Local Authority or another relevant body.

## **22. Records Relating to Staff Who Leave**

When an employee leaves the school:

- school records in their possession must be returned;
- access to school systems will be removed in accordance with agreed procedures;
- important business records held within their accounts or folders must be transferred to an appropriate location;
- school information must not be retained on personal devices or personal accounts; and
- relevant employment records will be retained in accordance with the Record Retention Schedule.

The school may retain or access business records within a former employee's school account where necessary and lawful for legitimate school purposes.

## **23. Training and Awareness**

Staff will receive appropriate information and training about records management and data protection relevant to their roles.

This will include, as appropriate:

- secure handling of information;
- record creation;
- retention and disposal;
- information sharing;
- cyber security;
- information rights;
- safeguarding records; and
- reporting information incidents.

Staff with specialist responsibilities may receive additional training.

## **24. Related Policies and Documents**

This policy should be read alongside the school's:

- Record Retention Schedule;
- Data Protection Policy and Privacy Notices;
- Freedom of Information Publication Scheme and Guide to Information;
- Child Protection and Safeguarding Policy;
- Low-Level Concerns Policy;
- Allegations Against Staff procedures;
- SEND Policy;
- Accountable Use of ICT, Online Services and Digital Technology Policy;

- 
- Acceptable Use of Mobile Phones, Cameras and Image-Recording Devices Policy;
  - Online Safety Policy;
  - CCTV arrangements/privacy information;
  - Complaints Policy;
  - Health and Safety Policy;
  - Staff Code of Conduct;
  - Finance Policy and financial procedures; and
  - relevant HR and employment procedures.

## **25. Monitoring and Review**

The school will monitor its records-management arrangements and take action where:

- records are being retained unnecessarily;
- records cannot readily be located;
- inappropriate duplication occurs;
- systems or working practices change;
- information incidents identify weaknesses;
- legislation or guidance changes; or
- the Record Retention Schedule requires amendment.

The school will periodically review the personal information it holds and securely erase or anonymise information that is no longer required. This reflects the current ICO storage-limitation principle.

This policy will be formally reviewed every two years, or sooner where necessary.