

Data Protection 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.

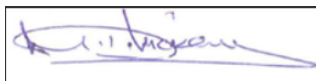
Document Control

<u>Item</u>	<u>Detail</u>
Policy Author	Helen Benarous/Headteacher
Policy Owner	Headteacher
Approval	Governing Board
Date Ratified	Autumn 2026
Review Cycle	
Next Review Due (or sooner if statutory guidance)	

Signatures

<u>Role</u>	<u>Name</u>	<u>Signature</u>	<u>Date</u>
Headteacher	Helen Benarous		21.8.26

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 and Scope

Templars Primary School is committed to protecting personal data and respecting the privacy rights of pupils, parents and carers, staff, governors, volunteers, visitors and other individuals whose information we process.

This policy explains how the school complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other applicable data protection requirements. It applies to personal data processed in any format, including electronic and paper records, images, recordings and information held within school systems.

The school is the Data Controller for personal data for which it determines the purposes and means of processing. Where another organisation is the controller, joint controller or processor, responsibilities will be determined by the relevant legal and contractual arrangements.

2. Data Protection Principles

The school will process personal data in accordance with the data protection principles. Personal data must be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not further processed incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary; and
- processed securely using appropriate technical and organisational measures.

The school is responsible for, and must be able to demonstrate, compliance with these principles.

3. Roles and Responsibilities

3.1 Governing Board

The Governing Board has overall responsibility for ensuring appropriate data protection governance and oversight.

3.2 Headteacher

The Headteacher acts as the school's day-to-day representative of the Data Controller and is responsible for ensuring that appropriate systems, policies and procedures are implemented.

3.3 Data Protection Officer

The school's Data Protection Officer is SchoolPro TLC Limited. The DPO advises the school on its obligations, monitors compliance, supports Data Protection Impact Assessments and acts as a



contact point for individuals and the Information Commissioner's Office. The DPO can be contacted at DPO@SchoolPro.uk.

3.4 All Staff

All staff are responsible for complying with this policy, relevant procedures and data protection training. Staff must protect personal data, only access information required for their role, use approved systems and report suspected personal data breaches promptly.

3.5 Data Processors

Where the school appoints an external organisation to process personal data on its behalf, it will undertake appropriate due diligence and ensure that a compliant written contract or other legal arrangement is in place.

4. Personal Data

Personal data is information relating to an identified or identifiable living individual. It may include names, contact details, identification numbers, online identifiers, attendance, assessment information, photographs and other information which identifies or can reasonably be linked to an individual.

The school processes personal data about pupils, parents and carers, employees, applicants, governors, volunteers, visitors and other individuals where necessary for its educational, safeguarding, employment, administrative and statutory functions.

5. Lawful Bases for Processing

The school will identify and document an appropriate lawful basis under Article 6 UK GDPR before processing personal data. Depending on the purpose, this may include:

- processing necessary to comply with a legal obligation;
- processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority;
- processing necessary for a contract or steps requested before entering a contract;
- processing necessary to protect someone's vital interests;
- legitimate interests, where this lawful basis is available and appropriate; or
- consent, where consent is the appropriate lawful basis.

The school will not rely on consent where another lawful basis more appropriately reflects the nature of the processing. Where consent is relied upon, it must be freely given, specific, informed and unambiguous and may be withdrawn.

6. Privacy Information and Transparency

The school will provide appropriate privacy information explaining how and why personal data is processed. Privacy notices will be reviewed and updated where processing changes materially.

Where personal data is obtained from another source, the school will provide privacy information where required unless an applicable exemption applies.

7. Special Category and Criminal Offence Data

7.1 Special Category Personal Data

Special category personal data includes personal data revealing or concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data used for unique identification, health, sex life or sexual orientation.

Templars Primary School does not currently process biometric data for the purpose of uniquely identifying individuals.

7.2 Criminal Offence Data

Criminal offence data includes personal data relating to criminal convictions and offences, related security measures, alleged commission of offences and proceedings relating to offences committed or alleged to have been committed.

7.3 Our Processing of Special Category Personal Data and Criminal Offence Data

As part of our statutory functions, Templars Primary School processes special category personal data and criminal offence data in accordance with the UK GDPR and the Data Protection Act 2018.

Because of the particularly sensitive nature of this information, the school will only process special category or criminal offence data where:

there is a clear and lawful purpose for doing so;
an appropriate lawful basis under Article 6 UK GDPR has been identified;
an additional Article 9 condition is identified where special category data is processed;
the requirements of Article 10 and the Data Protection Act 2018 are met where criminal offence data is processed;
the processing is necessary and proportionate; and
appropriate technical and organisational safeguards are in place.
The school processes special category and criminal offence data for purposes including its responsibilities relating to education, safeguarding, employment, equality, health and safety, and the protection and support of pupils and staff.

Where required by Schedule 1 of the Data Protection Act 2018, the school maintains a separate Appropriate Policy Document – Special Category and Criminal Offence Data. This identifies the relevant Schedule 1 conditions relied upon by the school and explains compliance with the data protection principles, protection of the information, retention and erasure arrangements and accountability arrangements.

Detailed retention periods are set out in the school's Record Retention Schedule. Further information about the categories of personal data processed, purposes and applicable lawful bases is provided in the school's relevant privacy notices and Record of Processing Activities.

Staff must seek advice from the Data Protection Officer where they are unsure whether special category or criminal offence data may lawfully be collected, used, disclosed or otherwise processed.

8. Sharing Personal Data

The school may share personal data where this is lawful, necessary and proportionate. Before sharing information, staff should consider the purpose, lawful basis, minimum information required, intended recipient and appropriate method of secure transfer.

Personal data may be shared with organisations including the Department for Education, Local Authority, health services, social care, police, safeguarding partners, examination or assessment bodies, professional advisers, service providers and other organisations where the school has a lawful basis to do so.

Nothing in data protection law prevents appropriate information sharing for safeguarding purposes. Staff must follow the school's safeguarding procedures and should not allow uncertainty about data protection to delay necessary safeguarding action.

9. Data Subject Rights

Individuals have rights under data protection law. Depending on the circumstances and lawful basis, these may include rights to:

- be informed about processing;
- access personal data;
- rectify inaccurate or incomplete personal data;
- request erasure;
- request restriction of processing;
- data portability;
- object to processing; and
- rights relating to automated decision-making and profiling.

Some rights are subject to legal conditions, exemptions or restrictions. Requests should be referred promptly to the appropriate school lead and/or DPO so that statutory timescales can be met.

10. Subject Access Requests

Individuals may request access to their personal data. Requests do not have to use a particular form or wording and may be made verbally or in writing.

Staff who receive a request that may constitute a subject access request must pass it promptly to the appropriate school lead. The school may take reasonable steps to verify identity and clarify the scope of a request where necessary.

The school will respond within the applicable statutory timescale and may extend that period where the law permits. Information relating to other individuals will be considered carefully and exemptions will be applied where appropriate.

11. Children's Data and Requests

Children have data protection rights in their own right. The school will consider a child's competence and the circumstances when deciding whether a child can exercise those rights independently or whether a person with parental responsibility may act on the child's behalf.

Safeguarding and the best interests of the child will be considered where relevant.

12. Accuracy and Record Keeping

Staff must take reasonable steps to ensure that personal data is accurate and appropriately updated. Records should distinguish between fact, professional opinion and allegation where this is relevant.

The school will maintain appropriate documentation of its processing, including its Record of Processing Activities, privacy notices, lawful bases, data-sharing arrangements, processor contracts, DPIAs, breach records and retention arrangements.

13. Retention and Disposal

Personal data will not be kept for longer than necessary. Detailed retention periods are set out in the school's Record Retention Schedule and should be read alongside the Records Management Policy.

When information reaches the end of its required retention period, it will be securely destroyed or permanently anonymised unless there is a lawful reason for continued retention.

Legal holds, safeguarding requirements, complaints, litigation, investigations or other lawful reasons may require records to be retained beyond their usual period. Such departures should be documented where appropriate.

14. Data Security

The school will implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.

Measures may include:

- role-based access controls and least-privilege access;
- strong passwords and multi-factor authentication where appropriate;
- secure school-approved systems and devices;
- encryption where appropriate;
- physical security for paper records and equipment;
- secure transfer and sharing methods;
- backups and resilience arrangements;
- staff training and confidentiality requirements;
- appropriate processor contracts and due diligence; and
- secure disposal of records and equipment.



Staff must comply with the Accountable Use of ICT, Online Services and Digital Technology Policy and other relevant information-security procedures.

15. Removable Media and Portable Storage

The use of USB sticks and other removable storage devices for school information is prohibited unless an exceptional use has been specifically authorised by the Headteacher or School Business Manager following appropriate information-security advice.

School information should be stored and transferred using approved school systems. Where exceptional removable-media use is authorised, appropriate encryption and other safeguards must be applied.

16. Personal Data Breaches

A personal data breach is a security breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

All suspected or actual personal data breaches must be reported immediately in accordance with the school's Data Breach Procedure. Staff must not delay reporting while attempting to investigate or resolve the matter themselves.

The school will assess the risk to individuals and, where required, notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of becoming aware of the breach. Where a breach is likely to result in a high risk to individuals, affected individuals will also be informed where required.

The school will maintain a record of personal data breaches, including decisions about notification.

17. Data Protection Impact Assessments

The school will undertake a Data Protection Impact Assessment before processing that is likely to result in a high risk to individuals' rights and freedoms, particularly where new technologies or significant new uses of personal data are proposed.

Staff introducing a new system, service, technology or significant change in processing must consult the DPO or appropriate school lead at an early stage so that privacy and data protection can be considered by design and by default.

18. International Transfers

Personal data will only be transferred outside the United Kingdom where the transfer complies with UK data protection law.

The school will ensure that an appropriate transfer mechanism or safeguard is in place where required. This may include UK adequacy regulations, the UK International Data Transfer Agreement,



the UK Addendum to approved EU Standard Contractual Clauses, or another lawful transfer mechanism.

Staff must not independently use overseas-hosted services to process school personal data unless the service has been approved through the school's procurement, data-protection and information-security arrangements.

19. CCTV, Images and Recordings

Where the school uses CCTV, photographs, video, audio or other recordings containing personal data, these will be processed for specified lawful purposes and in accordance with relevant privacy information and school policies.

Staff must comply with the Acceptable Use of Mobile Phones, Cameras and Image-Recording Devices Policy and must not use personal devices or accounts to capture, store or share pupil information except where explicitly authorised under school procedures.

20. Freedom of Information and Other Legal Duties

Data protection legislation operates alongside other legal duties, including freedom of information, safeguarding, education, employment and records-management requirements. Where requests engage more than one legal regime, the school will seek appropriate advice and apply the relevant requirements.

21. Complaints

Individuals who have concerns about how the school has processed their personal data should raise the matter with the school in the first instance and may contact the Data Protection Officer at DPO@SchoolPro.uk.

Individuals also have the right to complain to the Information Commissioner's Office. The school will provide appropriate contact information through its privacy notices and correspondence.

22. Training and Awareness

Staff will receive appropriate data-protection and information-security training and updates relevant to their roles.

Staff must complete required training, follow school procedures and seek advice where they are uncertain about the lawful or secure handling of personal data.

23. Monitoring and Review

The school will monitor compliance through appropriate governance, audits, incident review, staff training, DPO advice and review of policies and processing arrangements.



This policy will be reviewed annually and sooner where legislation, regulatory guidance, school systems or processing activities change materially, or where an incident identifies a need for revision.

24. Related Policies and Documents

Appropriate Policy Document – Special Category and Criminal Offence Data;
Records Management Policy;
Record Retention Schedule;
relevant Privacy Notices;
Record of Processing Activities;
Data Breach Procedure;
Child Protection and Safeguarding Policy;
Staff Code of Conduct;
Accountable Use of ICT, Online Services and Digital Technology Policy;
Acceptable Use of Mobile Phones, Cameras and Image-Recording Devices Policy;
Social Media and Online Communication Policy for Staff;
Freedom of Information Publication Scheme;
CCTV/privacy arrangements where applicable; and
relevant Data Protection Impact Assessments.