BUCKINGHAMSHIRE COUNCIL

Data Protection Policy
Tylers Green Middle School

This policy was adopted on: Summer 2026

The policy is to be reviewed by: Summer 2028

1. Aims

Our school aims to ensure that all data collected about staff, students, parents, and visitors is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR). This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of Data Protection Legislation, and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department for Education;

UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Data Protection Act 2018 (DPA 2018)

This policy is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.

This policy also covers requirements of Keeping Children Safe in Education 2023 (KCSIE 2023) paragraphs 141 and 142 Filtering and Monitoring.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified
Sensitive personal data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature • Where a person is a member of a trade union • Physical and mental health

	• Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions
Processing	Obtaining, recording, storing, altering or destruction of data
Data subject	The living individual whose personal data is held or processed
Data controller	A person or organisation that determines the purpose for which, and the way personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4. The Data Controller

Our school processes personal information relating to students, staff, parents, students' emergency contacts and visitors, and, therefore, is a data controller. The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5. Data Protection Principles

The UK GDPR is based on the following data protection principles, or rules for good data handling:

- data shall be processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK

GDPR in order to safeguard the rights and freedoms of individuals.

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6. Roles and responsibilities

The Governing Body has overall responsibility for ensuring that the school complies with its obligations under the UK GDPR. Day-to-day responsibilities rest with the Headteacher. The Headteacher will ensure that all staff are aware of their data protection obligations, and oversees any queries related to the storing or processing of personal data. Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address. Data breach reporting is mandatory under the UK GDPR, and all staff are aware of their obligation to report data breaches without delay.

7. Privacy/Fair Processing Notice

7.1 Students and parents

We hold personal data about students to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about students from other organisations including, but not limited to, other schools, Local Authorities, the Department for Education and the National Health Service. This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on student characteristics, such as ethnic group or Special Educational Needs and Disabilities
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about students with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this Policy.

We are required, by law, to pass certain information about students to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations.

7.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- enable individuals to be paid
- facilitate safer recruitment practice
- support the effective performance management of staff
- improve the management of workforce data across the education sector
- inform our recruitment and retention policies
- allow better financial modelling and planning
- enable monitoring of people with, and without, Protected Characteristics under the Equality Act
- support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited to, information such as:

- contact details, next of kin
- National Insurance numbers
- salary information
- qualifications
- absence data
- personal characteristics/protected characteristics
- medical information
- outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to. This may include advisers such as our Occupational Health and our Human Resources advisers. We are required, by law, to pass certain information about staff to specified external bodies, such as our Local Authority and the Department for Education, so that they can meet their statutory obligations. Any staff member wishing to see a copy of information about them that the school holds should contact the Headteacher.

8. Subject Access Requests

Under the UK GDPR, staff, students and parents\carers have a right to request access to information the school holds about them. This is known as a Subject Access Request.

Subject Access Requests must be submitted in writing, either by letter or email. Requests should include:

- The subject's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to Subject Access Requests:

- Information that might cause serious harm to the physical or mental health of the subject or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject Access Requests for all or part of the student's educational record will be provided within 15 school days. If a Subject Access Request does not relate to the educational record, we will respond within 1 calendar month. We reserve the right to charge for requests which are deemed to be excessive.

9. Parental Requests to see the Educational Record

Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of Subject Access rights. For a parent to make a subject access request, the child must either be unable to understand their rights and the implications of a Subject Access Request or have given their consent.

The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 and above as mature enough to understand their rights and the implications of a Subject Access Request. If parents ask for copies of information, they may be required to pay the cost of making the copies.

10. Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the school of a change of circumstances his/her computer records will be updated as soon as is practicable.

Data Checking Sheets for students will be provided to data subjects so they can check its accuracy and make any amendments on entry to Year 3. For Staff Data Checking Sheets will be issued every 12 months.

Where a data subject challenges the accuracy of his/her data the school will immediately mark the record as potentially inaccurate, or "challenged". In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Governing Body under the formal Complaints Procedure.

11. Artificial Intelligence

Tylers Green Middle School acknowledges that while artificial intelligence (AI) can enhance learning and efficiency, it also poses risks to personal and sensitive data. Key points from the school's approach include:

- Data Security: Entering personal or sensitive data into unauthorized generative AI tools or chatbots is strictly prohibited.
- Data Breaches: Any unauthorized entry of personal/sensitive data into an AI tool will be treated as a data breach according to the school's procedures.
- Risk Mitigation: AI-related risks are managed through existing policies, which are updated as necessary.
- Education: The school provides training for staff and students on the safe and ethical use of AI.

For more detailed information, please refer to the school's full Artificial Intelligence Policy.

12. Storage of Records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office. Staff must adhere to school policies and procedures when taking data off site.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, online resources, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops

and USB devices as far as is possible. Encryption, anonymisation and pseudonymisation will be used to protect the data.

- Staff, students or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.
- Governors are required to use school email addresses and use cloud storage for sharing information and data.
- UK GDPR compliant cloud storage will be used for all online data storage.

13. Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

14. Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. If a data breach is detected the school will follow the procedure adopted.

All data breaches are reported to the Data Protection Lead who liaises with the appointed Data Protection Officer. When appropriate, data breaches are escalated to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

15. Training

Our staff and governors are provided with data protection training as part of their induction process, and this is refreshed annually. Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary to keep staff up to date.

16. Monitoring Arrangements

The Head Teacher is responsible for monitoring and reviewing this policy. The school's Data Protection Lead checks that the school complies with this policy. This document will be reviewed if the General Data

Protection Regulation changes or otherwise every 2 years. At every review, the policy will be shared with the Governing Body or its delegated committee.

17. Links with other policies

This Data Protection Policy is linked to:

- Artificial Intelligence Policy
- Remote Education Policy
- Data Retention Policy
- The Freedom of Information Publication Scheme
- Privacy Notice (Student and Parent)
- Privacy Notice (Staff)

18. Contact

If you would like to discuss anything in this policy, in the first instance please contact the School lead below:

Position	Name	Email	Phone
School lead	Josephine Rutter	dpo@tylersgreenmiddle.co.uk	01494 812465
Data Protection Officer	Turn It On	dpo@turniton.co.uk	01865 597620