Last review: March 2026
Review date: March 2027
Signed: NC/PN/EV
Approval Committee: Governing Body

DATA PROTECTION GDPR POLICY

INCLUDING GILLINGHAM SCHOOL PRIVACY NOTICE

Gillingham School

Hardings Lane, Gillingham

Dorset, SP8 4QP

Data Protection: Gillingham School holds the legal right and obligation to collect and use personal data relating to students and their families as set out in the General Data Protection Regulations (GDPR). Under GDPR, the lawful basis we rely upon for processing student information are legal obligation, public task and substantial public interest.

Under GDPR there are six data protection principles that we will adhere to:
1) We will process data in a fair, lawful and transparent manner.
2) We will collect data for specified, explicit and legitimate purposes and it will not be further processed in a manner that is incompatible with those purposes.
3) We will collect an amount of data which is adequate, relevant and limited to what is necessary.
4) We will collect data accurately and where necessary keep it up to date
5) We will keep data in a form permitting identification for no longer than is necessary.
6) We will process data in a manner ensuring appropriate security of personal data.

Underpinning these principles, individuals have five main rights within GDPR, centered around:

1. To access their data
2. To rectify their data (correcting data)
3. To erase their data
4. To restrict the processing of their data
5. To withdraw their consent for data use.

The Governing Body of the school has overall responsibility for ensuring that records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions. The Head Teacher and Governors of the School intend to comply fully with the requirements and principles of GDPR and both the Data Protection Act 1998 and the Data (Use and Access) Act 2025 which adds targeted amendments, modernizing them in line with technological advancements. All school staff are aware of their duties and responsibilities within these guidelines. This policy and general procedures are reviewed regularly and at least annually.

The Gillingham School **Privacy Notice** forms part of this policy and is available on the school website and should be considered as an Appendix to this document. This outlines 'Why and How' we process data and our legal basis for doing so.

Please also see the **Biometric Information Policy**.

<u>Data accuracy</u>
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, their computer (SIMS) record will be updated as soon as it is practicable. Updated student data can also be communicated to the school using the Edulink App/website.

<u>Data Retention</u>
Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of administrative staff, Year Heads, Heads of Department and Senior

Staff to ensure that obsolete data is properly erased and/or destroyed as appropriate, using the 'Retention Guidelines for Schools' documentation.

Data and Computer Security

Gillingham School undertakes to ensure security of personal data in the following ways:

1) Physical Security

- Appropriate building security measures are in place, such as alarms, window bars, deadlocks and computer hardware cable locks.
- Only authorised people are allowed in the computer server rooms.
- Files and other personal data are stored securely when not in use.
- Visitors to the school are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

2) Electronic Security

- Clear data protection is closely linked to cyber security, and we will be mindful of the advice in the '10 Steps to Cyber Security' leaflet produced by the National Cyber Security Centre.
- Gillingham School uses various in-perimeter and out-of-perimeter security systems to mitigate against ransomware, malware and viruses.
- Staff training, advice and guidance on e-security are available from the IT Services Department in school.
- Security software is installed on all computers containing personal data.
- Only authorised users are allowed access to the computer files.
- Computer files are 'backed up' regularly.
- Clearly, many documents in school contain sensitive and personal data. (For example, EHCPs, SEN statements and annual reviews, exclusion letters). Great care must be taken when, on very rare occasions, copies of these documents are taken off-site.
- Use of memory sticks is strongly discouraged, and any containing of personal and sensitive data should be encrypted and documents protected. Technical assistance with this is available from the IT Services Department in school. Staff are advised to use remote access to view data away from the school, rather than transporting data via a memory stick.
- Staff must ensure that when staff or pupils' information (electronically or otherwise) is taken off site it is always kept secure.

3) Procedural Security

- All staff are informed of their Data Protection obligations and their knowledge updated as necessary. Staff are regularly reminded about their responsibilities regarding GDPR.
- Staff are aware that individuals can be personally liable in law under the terms of the Data Protection Acts and that a deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.
- To be given authorised access to the computer, staff will have to undergo checks and will agree to a confidentiality agreement (this is done when staff log on to the computer).
- Staff should not leave their computers logged on to personal data (for example, SIMS)

when they are not present in the room. Use of 'Windows' 'L' to lock a workstation is encouraged.

- Printouts as well as source documents containing personal data are stored securely and shredded before disposal according to our retention schedule. (For example, personal data recorded for school trips). Where possible, staff should avoid printing documents containing personal data.
- Students' school record files should not be taken off-site except under exceptional circumstances.
- Staff should avoid leaving documents containing personal and sensitive data in places easily seen by others; for example, they are left on desks at the end of the day.
- Staff should take extra care to ensure that emails are sent to the intended recipient only.
- As outlined in the school's Privacy Policy, we will ensure that any 'third party' contractors handling data are GDPR compliant. When data is required to be shared, the same data protection standards that Gillingham School upholds are imposed on the processor. The minimum amount of data is transferred, such as student name and date of birth, as necessary.
- When mandatory the school will ensure to have a Data Protection Impact Assessment in place. Instances where this applies are the use of CCTV, the use of CCTV in washrooms and the use of biometrics. A summary of these documents is available on request.
- Gillingham School have considered the need for using CCTV and have decided it is necessary to help deter crime, protect the safety of individuals, or the security of premises. We will not use the system for any incompatible purposes, and we conduct regular reviews of our use of CCTV to ensure that it is still necessary and proportionate. Gillingham School notifies all pupils, staff, and visitors of the purpose for collecting CCTV images via signage and letters. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose. All CCTV footage may be kept for 30 days for security purposes; a nominated controller is responsible for keeping records secure and allowing access to images. These will be viewed on a case-by-case basis and only when appropriate. 22 Under Article 15 of the UK GDPR law, the right of access gives individuals the right to obtain a copy of their personal data from CCTV unless an exemption applies. This can be provided either in permanent form, or through arrangement to view the information. An exemption would include if the footage included other people. This will then need to redact so they cannot be identified. Where this is not possible or appropriate, we will consider asking for their consent before releasing this. Where this is not possible or appropriate, we will balance the requester's rights against any third-party rights to privacy and decide if it's reasonable to share the footage without their consent. The reasons for any decision will be documented.
- At present the school does not use any Automated Decision-Making systems without human intervention but will keep this under review and incorporate guidance when it becomes necessary.

- Marketing and Cookies. We comply with PECR rules for electronic marketing and cookies. When DUAA cookie changes commence, certain low‑risk cookies (e.g., statistical or functionality) may be set without prior consent, provided we meet transparency and opt‑out requirements; keep banners/notices under review. PECR fines now align with UK GDPR.
- Use of Artificial Intelligence (AI). Our school may make use of artificial intelligence (AI) tools to support teaching, learning, and administrative functions. Any use of AI will comply with the UK GDPR and Data Protection Act 2018.
    - Personal or sensitive data must **not** be entered into AI systems unless a Data Protection Impact Assessment (DPIA) has been completed and appropriate safeguards are in place.
    - AI tools will only be used following assessment of risks relating to accuracy, fairness, transparency and data security.
    - All AI-generated content will be reviewed by staff before use.
    - No automated decision-making that produces legal or significant effects on individuals will be carried out using AI.

This aligns with DfE and ICO expectations and current sector practice.

Subject Access Requests

Data subjects have a right to access their own personal data. To ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Requests from pupils will be processed as any subject access request as outlined below and the copy will be given directly to the pupil, unless the pupil does not understand the nature of the request. Requests from pupils who do not appear to understand the nature of the request will be referred to by their parents or carers.
Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent when appropriate.

Processing Subject Access Requests

Requests for access must be made in writing.

Pupils, parents or staff should ask for a Data Subject Access form, available from Mrs. A Stickland. Completed forms should be returned to her. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access Log book, showing the date of receipt, the data subject's name, the name and address of requester (if different), the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 20 working days, therefore not including school holidays, from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided. A

reasonable charge will be incurred to cover the costs of photocopying.

In the case of any written request from a parent regarding their own child's record, access to the record will be provided in accordance with the current Education (Pupil Information) Regulations.

Disclosure of Data

A "legal disclosure" is the release of personal information to someone who requires the information to do his or her job within or for the school.

An "illegal disclosure" is the release of information to someone who does not need it, or has no right to it, or one which falls outside the school's registered purposes. It is worth noting that comments on Facebook / Twitter etc. which disclose privileged personal data would fall into the category of 'illegal disclosure'. As required under GDPR, we will report a data breach / illegal disclosure to the ICO within 72 hours where the loss of data is more than likely 'to result in a risk to the rights and freedoms of natural persons', for example damage to reputation, financial loss or discrimination. We will also inform the individuals involved.

Contacts in school are Ms. E Vallender (Data Protection Officer), Mrs. A Stickland (Headteacher's PA) and Mrs. N Cross (Assistant Headteacher). General information about General Data Protection Regulation (GDPR) and The Data Protection Act can be obtained from the Information Commissioner's Office (ICO), (website www.ico.org.uk)

Gillingham School Privacy Notice
(Why and how we use student information)

Gillingham School is the data controller of the personal information you provide to us. This means the school determines the purposes for which, and the manner in which, any personal data relating to students and their families is to be processed.

In some cases, your data will be outsourced to a third-party processor; however, this will only be done with your consent, unless the law requires the school to share your data. Where the school outsources data to a third-party processor, the same data protection standards that Gillingham School upholds are imposed on the processor.

Ms. Emma Vallender is the data protection officer. Their role is to oversee and monitor the school's data protection procedures, and to ensure they are compliant with GDPR (General Data Protection Regulation).

Why we collect and use this information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to provide appropriate pastoral care

- to assess the quality of our services
- to comply with the law regarding data sharing
- to safeguard students

Our Legal Basis to Process Data

Gillingham School holds the legal right to collect and use personal data relating to students and their families, and we also receive information regarding them from their previous school, Local Authority and the Department for Education.
Under GDPR, the lawful bases we rely on for processing pupil information **are legal obligation, public task and substantial public interest.**
We collect and use personal data to meet legal requirements and legitimate interests set out in GDPR and UK law, including those in relation to the following:

- Article 6 and Article 9 of the GDPR: Processing of personal and special category data is necessary due to a legal obligation and substantial public interest.
- Regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address, parent/guardian, contact details)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information
- Medical and administration (such as doctors' information, child health, dental health, allergies, medication and dietary requirements)
- Special Educational Needs and Disability
- Behaviour and exclusions
- Education/school history
- Siblings' information
- Safeguarding information (such as court orders and professional involvement)
- Identity management, such as school photographs & CCTV
- Free School Meals & Pupil Premium management
- Trips and activities

How we collect pupil information

Pupil data is essential for the schools' operational use. We collect pupil information via Admission Forms, Edulink, Common Transfer Files (CTF) and other information which you send to the school.

Whilst the majority of pupil information you provide to us is mandatory, some of it is requested on a voluntary basis. To comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if your consent is needed. Where consent is required, we will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. For most students this will be until the year of their 25th birthday, as set out in the Dorset Local Authority retention schedule. However, we are required to retain some Special Educational Needs and Disability information for longer than this. Student files are stored securely and paper files destroyed by secure collection and incineration.

Who we share pupil information with

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.
We routinely share pupil information with:

- Schools that the students attend after leaving us
- Our Local Authority (Dorset County Council)
- Other Local Authorities in which our students live (Wiltshire, Somerset)
- Youth support services (students aged 13+)
- The Department for Education (DfE)
- Exam Boards
- The Education and Skills Funding Agency
- Aspens (School Catering providers)
- School transport companies
- Curriculum resource providers, such as GCSEPod and Sparx.
- NHS, the school nurse and other health professionals as necessary

Data (such as student names) may be shared with educational websites to enable students to log in to these in lessons or for home learning.

When data is required to be shared, the same data protection standards that Gillingham School upholds are imposed on the processor. The minimum amount of data is transferred, such as student name and date of birth, as necessary.

The Learning Records Service (LRS)

The information you supply is used by the Learning Records Service (LRS). The LRS issues Unique Learner Numbers (ULN) and creates Personal Learning records across England, Wales

and Northern Ireland, and is operated by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE). For more information about how your information is processed, and to access your Personal Learning Record, please refer to: https://www.gov.uk/government/publications/lrs-privacy-notices

Youth support services

Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

- Post-16 education and training information
- Youth support services
- Careers advisers

For more information about services for young people, please visit our local authority website.

.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our students with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under Section 3 of The Education (Information About Individual Students) (England) Regulations 2013.
All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual

Students) (England) Regulations 2013. The DfE may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- Conducting research or analysis
- Producing statistics
- Providing information, advice or guidance

Sharing by the Department for Education (DfE)

The law allows the Department to share students' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

Requesting access to your personal data

Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs Emma Vallender (Data Protection Officer) at the school.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- have inaccurate personal data rectified, blocked, erased or destroyed
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance.

Contact

If you would like to discuss anything in this Privacy Notice, please contact Ms Emma Vallender (Data Protection Officer) at the school.