Last review: September 2020
Review date: September 2021
Signed By:
Approval Committee: Governing Body

GILLINGHAM SCHOOL
Hardings Lane, Gillingham
Dorset SP8 4QP

GILLINGHAM SCHOOL DATA PROTECTION (GDPR) POLICY

Gillingham School Data Protection (GDPR) Policy

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 bases we rely on 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, centred 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 the Data Protection Act 1998. 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 alongside this document. This outlines 'Why and How' we process data and our legal basis for doing so.

.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 their computer (SIMS) record will be updated as soon as is practicable. Updated student data can also be communicated to the school using the SIMS ParentLite App.

Retention of Data

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 persons 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

- Clearly 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.
- 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.
- Memory sticks containing personal and sensitive data should be encrypted and documents password-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 pupil information (electronic or otherwise) is taken off site that it is kept secure at all times.

3) Procedural Security

- All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Staff are regularly reminded about their responsibilities with regards to 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.
- In order to be given authorised access to the computer, staff will have to undergo checks and will agree 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)
- 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, left on desks at the end of the day
- 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.

Subject Access Requests

Data subjects have a right of access to their own personal data. In order 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 it is clear that 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 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 may ask for a Data Subject Access form, available from the School Office. Completed forms should be submitted to Mrs A Stickland. 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 30 days 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 date on which sufficient information has been provided.

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 Mr K Barker (Deputy 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)