Last review: March 2024
Review date: March 2025
Signed By:
Approval Committee: Governing Body

GILLINGHAM SCHOOL
Hardings Lane, Gillingham
Dorset SP8 4QP

GILLINGHAM SCHOOL DATA PROTECTION (GDPR) POLICY (INCLUDING GILLINGHAM SCHOOL PRIVACY NOTICE)

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, 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**.

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 Edulink App/website.

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.
- 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 is 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 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). 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, 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.

- 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 redacted 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.

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 should 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 working 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)

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.

Mrs 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 in order 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 requested on a voluntary basis. In order 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 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 Hegarty Maths.
- 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 Mrs Emma Vallender (Data Protection Officer) at the school.

Gillingham School Staff Data Protection Guidance

There is a massive amount of personal data in school, stored electronically and on paper, and it is our **legal duty** to keep that data safe and ensure that it is only seen by those entitled to see it.
Our Data Protection Officer is Emma Vallender, who has an overview of all our processes and procedures, but **we are ALL responsible for keeping data secure**.

So, a few reminders:

You should:	**Please DO NOT:**
Lock your laptops / workstations ('Windows' 'L') when you are not in the room. If checking emails- make sure your screen is not being projected.	Leave SIMS, email etc. open in your classroom / office when you are not in the room.
Think about what information you are leaving on your desk, including overnight.	Leave confidential information / personal data on your desk overnight or on show on your desk when you are not in your classroom. This includes student lists if they have any data on them (PP, SEN etc.)
Memory sticks / removable storage are HIGH RISK! If you need to use a memory stick it will require encryption. See the IT support team if you need help with this.	Load school data onto unencrypted computers at home or email student personal data via email to home.
It is best to use remote access to view data away from the school, rather than transporting data via a memory stick.	Download school data to your home computer to work on it.
Ensure that your login details are secure by choosing a high level password.	Choose an insecure password such as 'secret', '1234' or 'ABCD'. See the IT support team if you need help with changing your password.
The PaperCut printing system should mean that unclaimed printouts will not be left in a copier for others to see.	Leave confidential documents on printers / copiers or in the repro room.
If you have student files stored in your office / classroom they must be kept in a locked filing cabinet or cupboard at all times.	Leave student files unsecured so they can be accessed without a key.
If you are emailing a group of parents/members of the public outside school (for example, sending the same email to several parents) use the BCC function. Go to 'Options > BCC' if it doesn't appear).	List all personal email addresses in the To: or CC: section of the email when responding to parents or other members of the public. Everyone will see everyone else's personal email address.
Check the person you are emailing is entitled to receive the data you are sending – how do you know?	Assume that a step parent has legal authority and send them data without checking.
Be particularly careful when exporting student data to a spreadsheet – they can contain thousands of items of personal data!	Share data in a spreadsheet format outside of school unless it is password protected.

If you are asked to disclose personal data over the telephone, check that the person you are talking to is really who they say they are. Ask two security questions, one about their details in SIMS and one about the child.	Do not give any information about a student over the telephone unless you can confirm the identity of the caller and they have permission. (Ask yourself what checks a bank will do before they will confirm that you have an account with them).
If you are organising a trip or visit, only collect the personal data which is required. Medical forms should be shredded immediately after the trip and consent forms passed to the Finance Office.	Leave confidential information provided for trips unsecured, or in the recycling / rubbish bin.
If you have Apps using personal data e.g. Edulink, on your smartphone/tablet/other device, please inform Josh / Ollie in IT Support immediately if your device is lost or stolen, so that your passwords can be reset as a matter of urgency.	Use exam scripts unless the student has given permission to do so - see Emma Addis (Exams) Please remove names from exam scripts before using
Please be wary of emails from an unexpected source which then ask you to enter your logon detail to access a link or attachment. This may be a scam to discover your login details, which for example could then be used to access the personal data sent in your school emails. Look for the padlock symbol (https:) in the web address which indicates a secure site. If in doubt about the authenticity of a request for details, please consult Josh/Scott for advice.	Sign up to websites which require student/parental data to be shared with external organisations. Please see IT services who will check GDPR policies
Check with IT Services before you sign up to a website which requires student data. Their Privacy Notice will need to be checked.	

GDPR Guidance for Staff in Non-teaching Roles

You should:	**Please DO NOT:**
Lock your laptops / workstations ('Windows' 'L') when you are not in the room. If checking emails- make sure your screen is not being projected.	Leave SIMS, email etc. open in your office when you are not in the room.
Think about what information you are leaving on your desk, including overnight.	Leave confidential information / personal data on your desk overnight or on show on your desk when you are not in your room. This includes student lists if they have any data on them (PP, SEN etc.)
Memory sticks / removable storage are HIGH RISK!	Load school data onto unencrypted computers at home or email student personal data via email to home.

If you need to use a memory stick it will require encryption. See the IT support team if you need help with this.	
It is best to use remote access to view data away from the school, rather than transporting data via a memory stick.	Download school data to your home computer to work on it.
Ensure that your login details are secure by choosing a high level password.	Choose an insecure password such as ‘secret’, ‘1234’ or ‘ABCD’. See the IT support team if you need help with changing your password.
The PaperCut printing system should mean that unclaimed printouts will not be left in a copier for others to see.	Leave confidential documents on printers / copiers or in the repro room.
If you have student files stored in your office / classroom they must be kept in a locked filing cabinet or cupboard at all times.	Leave student files unsecured so they can be accessed without a key.
If you are emailing a group of parents/members of the public outside school (for example, sending the same email to several parents) use the BCC function. Go to ‘Options > BCC’ if it doesn’t appear).	List all personal email addresses in the To: or CC: section of the email when responding to parents or other members of the public. Everyone will see everyone else’s personal email address.
Check the person you are emailing is entitled to receive the data you are sending – how do you know?	Assume that a step parent has legal authority and send them data without checking.
Be particularly careful when exporting student data to a spreadsheet – they can contain thousands of items of personal data!	Share data in a spreadsheet format outside of school unless it is password protected.
If you are asked to disclose personal data over the telephone, check that the person you are talking to is really who they say they are. Ask two security questions, one about their details in SIMS and one about the child.	Do not give any information about a student over the telephone unless you can confirm the identity of the caller and they have permission. (Ask yourself what checks a bank will do before they will confirm that you have an account with them).
Please be wary of emails from an unexpected source which then ask you to enter your logon detail to access a link or attachment. This may be a scam to discover your login details, which for example could then be used to access the personal data sent in your school emails. Look for the padlock symbol (https:) in the web address which indicates a secure site. If in doubt about the authenticity of a request for details, please consult Josh/Scott for advice.	Sign up to websites which require student/parental data to be shared with external organisations. Please see IT services who will check GDPR policies

- Ensure that all Data Protection issues/queries are referred to the Data Protection Officer EV.
- Ensure that any Subject Access Requests are referred on to AS as soon as is possible, because we need to respond within 20 working days.
- If asked to collate information for a Subject Access Request when documents are scanned the file name needs to be changed to a number and this number should be noted on the paper copy. If another student is named in any of the documentation their name must be redacted.
- Any blank templates should be saved to a particular folder. When sending a template to someone it needs to be checked to ensure that it is still blank.
- A parent on requesting exam certificates was in error given a book which contained personal data of students from that year group.
- Before using photographs of students in published items, social media or the school website ensure that we have permission to use them.
- Remove photographs from publications and school website when students are no longer at the school.
- We need to maintain a list of the records which have been destroyed and the person who authorised it.
- We need to keep a log of Subject Access Requests.
- If making a telephone call that involves sensitive or private information, make sure you are in a secure area or wearing headphones.

Gillingham School Internet Safety and IT Use: Acceptable Use Policy (Staff Version)

See also: Social Networking Policy, GDPR (Data Protection) Policy.

Introduction

The school's computers offer access to a vast amount of information for use in preparing and delivering lessons, offering great potential to support and enrich the curriculum. For example, the Internet is a wonderful resource providing information and excellent learning activities and opportunities; however, all schools have a duty to ensure that all students and staff access the Internet and other resources safely and responsibly. The following guidelines are to ensure that this is the case; please read them carefully. Each time that you log on to a school computer you are agreeing to keep to the rules, which are also in place for your own safety. The guidelines refer to all school computers, and any other school services consumed on any other devices, including but not limited to staff laptops being used outside of school, email on phones, remote access via the school gateway etc.

Security and Privacy

- Staff should never disclose their password to other colleagues, or use another colleague's password. Passwords should be changed from the default.
- Staff should not leave their computer unattended when still logged on; for example, confidential SIMS information may be accessed by an unauthorized individual. Staff should log off at the end of each session, or lock their computer if only away for a short time.
- Staff should use extreme caution when using a school computer to reveal their personal details, home address or telephone number on the web or in dialogue with other Internet users, and should only reveal this information if it is strictly necessary.
- The school computers must never be used in a way that harasses, harms, offends or insults others.
- The security in place on the computers should be respected; staff must not attempt to bypass or alter these settings in any way.
- Staff should be aware that computer storage areas, such as files and communications, may be viewed by IT support and senior management to ensure that the system is being used responsibly.

Internet

- Before publishing a photograph on the school website, or in a newsletter/prospectus, staff must also check whether parents have opted out of allowing their child's images to be displayed; the Librarian maintains an up-to-date list.
- Images of children on our website will not be labelled with their names.
- Staff must not allow students to engage in conversation or dialogue with other users on the Internet without permission or direct supervision.
- Staff must not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
- If a member of staff accidentally accesses inappropriate material, they should immediately report this to a member of the senior management team.
- Staff should not access social networking sites in school, except when necessary to teach e-safety or when social networking is part of the scheme of work.
- Staff should not discuss particular students on social networking sites, or make comments which may damage the school's reputation in the community.
- Staff must not use social networking sites (including Instagram) to communicate with current students. All settings should be set to 'private'.
- All Internet access at school is filtered through a proxy server to screen undesirable sites at source; this facility must only be disabled by a system administrator. If staff feel that particular sites are being filtered unnecessarily, they should contact IT Services, who will consider such requests.
- Staff should respect the work and ownership rights of people outside the school, as well as students and other staff. This includes abiding by copyright laws.
- All Internet and e-mail access is monitored at the school and if inappropriate behaviour is suspected, the Senior Leadership Team will be informed, and further action may ensue. Logs of Internet access are kept for all users of the network.

E-mail

- Email monitoring software is in use in the school, allowing IT staff to view all school emails. IT Services' staff regularly monitor any automatically blocked emails, and will release any that are unnecessarily blocked.
- Staff must not reveal their personal (home) e-mail addresses to students. The school e-mail addresses are able to be used for this purpose.
- Attachments to e-mails should not be opened unless they come from someone already known and trusted; they could contain viruses or other destructive programs.

- The sending or receiving of e-mail containing material likely to be unsuitable for children or schools is obviously prohibited. This applies to any material of a violent, dangerous, racist or other inappropriate nature. If such messages are received they should be reported to a member of IT support and senior management.

Cameras and other equipment

- All users of the school network are expected to print responsibly by not wasting expensive resources such as paper and particularly ink/toner.
- Any digital images, for example those taken during school trips, must be transferred to a secure location, for example on the school network (i.e. where pupils cannot access), as soon as possible and then deleted from the camera. This is particularly the case if staff are using their personal digital cameras. Photographs from school trips should not be published on social networking sites.
- Webcams should not be used in school unless specifically for teaching purposes.
- Mobile equipment (such as laptops, tablet PCs, PDAs, smartphones) should not be connected to the network unless they are healthy (free from viruses and malware) and their electrical systems are checked and marked for safety by a member of IT Services staff.
- Staff should not use their personal mobile phones to 'text' students.
- BYOD (Bring Your Own Devices), such as Smart 'Phones, laptops, iPads, etc., which connect to the school's Wi-Fi access points (where available), are subject to the same, or more rigorous filtering rules as school equipment.

Gillingham School IT Systems Acceptable Use Policy Agreement

I have read and understood the Acceptable Use Policy, and I agree to abide by the guidelines. I understand that any inappropriate or unlawful use of school IT facilities could lead to appropriate disciplinary of legal action being taken.

If these conditions are not followed, and inappropriate use of IT Systems is discovered / reported, this may result in disciplinary action. The Headteacher has a duty of care to report any inappropriate use of IT and Internet technology to the necessary authorities, including the Police in the case of illegal material.