



The Grey Coat Hospital

Online E-Safety Policy

POLICY NAME:	Online E-Safety Policy
GOV COMMITTEE:	Curriculum Committee
LAST POLICY REVIEW DATE:	May 2026
POLICY REVIEW TIMING:	Annual

Contents

1. Aims.....	3
2. Legislation and guidance.....	3
3. Roles and responsibilities.....	3
4. Educating pupils about online safety	5
5. Educating parents about online safety	6
6. Cyber-bullying	6
7. Acceptable use of the internet in school	8
8. Pupils using mobile devices in school	8
9. Staff using work devices outside school	8
10. How the school will respond to issues of misuse.....	8
11. Training.....	9
12. Monitoring arrangements.....	9
13. Links with other policies.....	10
Appendix 1: acceptable use agreement for Students.....	11
Appendix 2: acceptable use agreement staff, volunteers and authorised visitors	14

1. Aims

We aim is to have robust processes in place to ensure the online safety of pupils, staff, governors, volunteers and other authorised users. We will deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology. We have established clear mechanisms to identify, intervene and escalate an incident, where appropriate. In this fast moving area we will frequently assess our procedures to ensure we keep pace with industry best practice.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self harm, suicide, anti-Semitism, radicalisation and extremism

Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

[Teaching online safety in schools](#)

[Relationships and sex education](#)

[Searching, screening and confiscation](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's DSL and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
 - Working with the headteacher, Head of ICT Support and other staff, as necessary, to address any online safety issues or incidents
 - Managing all online safety issues and incidents in line with the school child protection policy
 - Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
 - Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
 - Updating and delivering staff training on online safety
 - Liaising with other agencies and/or external services if necessary
 - Providing regular reports on online safety in school to the headteacher and/or governing board
- This list is not intended to be exhaustive.

3.4 The Head of ICT Support

The Head of ICT Support is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a bi-weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here' .

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – [UK Safer Internet Centre](#)
- Hot topics – [Childnet International](#)
- Parent resource sheet – [Childnet International](#)
- Healthy relationships – [Disrespect Nobody](#)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

It is also taken from the [guidance on relationships education, relationships and sex education \(RSE\) and health education](#).

All schools have to teach:

- [Relationships education and health education](#) in schools
- [Relationships and sex education and health education](#) in

secondary schools In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- Recognise inappropriate content, contact and conduct, and know how to report concerns. (This includes racist, sexist, homophobic, transphobic, discriminatory, hateful, abusive, politically extremist content, content that promotes violence against others or oneself, radicalisation, illegal activity, any other forms of harmful behaviour.)

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity ➤ How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home. This policy will also be shared with parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with the headteacher.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying as part of the pastoral curriculum and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on [screening, searching and confiscation](#)
- UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, staff, volunteers and governors who will have access to the school systems must sign an agreement regarding the acceptable use of the school's ICT systems. Visitors will be expected to read and agree to the school's terms on acceptable and are required to do so in order to access the IT system.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them during the school day or before or after school while on the school premises.

In the unlikely event that a pupil will be given permission to use their phone, it must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil will trigger disciplinary action in line with the school behaviour policy, which will result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lowercase letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their work device, they must seek advice from the Head of ICT Support.

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and our ICT use agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, harassing, and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - Sharing of abusive images and pornography, to those who don't want to receive such content
 - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL, Deputy DSLs and other staff with concerns, logs behaviour and safeguarding issues related to online safety.

This policy will be reviewed regularly by the Governors' Curriculum Committee. At every review, the policy will be shared with the governing board. The review will be supported by a risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Bring Your Own Devices Policy
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy

Please note:

The Grey Coat Hospital ***Bring Your Own Devices Policy*** covers the conditions under which students may bring in their own laptop generally and during the examination period. Please read the Bring Your Own Devices Policy in conjunction with this Online E-Safety Policy.



The Grey Coat Hospital

ICT CODE OF CONDUCT AGREEMENT

Student's Name: _____ (in caps) Form (if known) _____

The ICT facilities at The Grey Coat Hospital offer students access to a vast range of information and software which supports the delivery of the curriculum at all key stages. The computers are provided and maintained for the benefit of all students, and they are expected to use the facilities responsibly. It is expected that equipment is treated respectfully so that it remains available for other users. Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Application of the code of conduct outside school

Students should be aware that any use of communications technology at home or elsewhere, which relates to school in any way (e.g. school work, emails or texts addressed to other members of the school community, or communications about the school, or about any members of the school community) are subject to this policy.

Social media guidance

The school name, badge, uniform and motto are the property of the school, and should not be used in any public form of communication on the internet or on Social Media sites. Students may not post on any social media sites, videos or movies taken in school or, of themselves or friends, wearing school uniform. Students should ensure their privacy settings and other available security is set at the highest level at all times for their personal protection.

Remember: Never post on a website or social media platform something which you might later regret or be embarrassed about or which breaks the school behaviour code.

Application of the code of conduct in school

School Equipment

- Always get guidance from any ICT Staff before installing and/or attempting to install or store programs of any type on the computers.
- Damaging, disabling, or otherwise harming the operation of computers and the hardware itself, or intentionally wasting resources, i.e. file duplication, is prohibited.
- Only use the computers for educational purposes. Any other activities are prohibited unless you have permission from your teacher to do so.
- Always check files brought in on all removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Where appropriate, always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Eating and drinking are prohibited near any of the ICT equipment.

Electronic Data

- Data available to students should only be accessed using privileges granted to students i.e. username, password, etc.
- All data on the network is protected by Symantec anti-virus software which runs on servers and workstations, and is updated automatically every day.

- Students should consult the school ICT Staff if they have or suspect a file is infected with any computer virus.
- When accessing the files on the school server from outside the school (via the school website), please make sure that your home computer also has anti-virus software installed which is regularly updated with the latest virus definitions.
- You should not intentionally delete or move a file from any public folder that does not belong to you.
- Students' data will be deleted by the end of summer term every year (except those in year 10 and 12 which will be deleted every 2 years). Students must save their own files on their personal external disk storage should they want to keep a copy of their work at the end of summer term.
- No file is retrievable once it has been deleted at the end of the summer term.

Security and Privacy

- Never disclose your username and password to anyone (including to your friends) and never use someone else's login name or password.
- Always log off whenever you have finished using a computer in school.
- Do not reveal your home address, telephone number, school name, or picture to anyone unless given permission by a teacher.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings is prohibited.
- Computer storage areas and removable media will be treated like school lockers. ICT staff may review your files and communications to ensure that you are using the system responsibly.

Internet

- All individual internet activities are recorded on the server and are checked on a regular basis.
- You are not allowed to use any computer with Internet access in the school without supervision from a member of staff.
- You should access the Internet only for study or for school authorised/supervised activities as instructed by your teacher.
- Chat rooms and other similar sites are prohibited. Never engage in exchanging messages with someone you do not know. You may be putting yourself at risk as young people are often targeted by those who have an unhealthy interest in children.
- Though the school does have an Internet filter, please make sure that you only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is prohibited.
- You must not download any electronic copyrighted and/or licensed-required files from any school computer, and laptops unless the school has the license to do so and you have been given permission by a teacher.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

Remote Learning

- All individual internet activities are recorded on the server and are checked on a regular basis.
- The recording of or photographing of your classmates or teachers during a remote live session is strictly prohibited.

- You need to be dressed appropriately for learning as you would be at school (no pyjamas for instance)
- You are not to turn on your camera, your face should not be visible during the live session.
- You can use the chat section to communicate during the live session only as instructed by your teacher.
- Your behaviour and conduct needs to adhere to the same expectations as those in a classroom and outlined in your diary. Failure to do so will result in contacting your parent(s)/carer and the risk of being banned from remote live sessions.

Email

- You will be provided with an email address by the School, and the expectation is that you will use this facility for legitimate educational and research activity.
- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street. Remember that you are a representative of the School on a global public system
- You should not open your email during lesson unless instructed by your teacher to do so.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate nature, always report such messages to your teacher or ICT Staff. The sending or receiving of any inappropriate email is strictly forbidden and will be viewed as misuse of resources and therefore will be dealt with according to the school's code of conduct.
- Avoid giving your email address or signing up to any inappropriate companies. When signing up to legitimate organisations, tick on the box which says "do not wish to receive any information from a trusted/selected third party companies".

Remember: Electronic mail is not guaranteed to be private so again, never write in an email something which you might later regret or be embarrassed about or which breaks the school behaviour code.

Other ICT rules will be added to the relevant headings as and when necessary. Students and carers will be notified of any updates to this policy. Students are obliged to follow these rules at all times.

Students and carers, please read this document carefully and sign below. Only once it has been signed and returned will access to the school ICT facilities be permitted. Access to the ICT facilities may be denied if this agreement is violated and additional action may be taken by the school in line with existing policies regarding school behaviour. For serious violations, a fixed term exclusion may be imposed. In certain circumstances, the police may be contacted or other legal action may be taken.

I confirm that I have read and understand the above and agree to use the school computer facilities within these guidelines.

Student signature: _____ **Date:** _____

I confirm that I have read and understood the above.

Parent/Carer Name: _____

Signature: _____ **Date:** _____



The Grey Coat Hospital

ICT AND CONFIDENTIALITY AGREEMENT

Staff Name: _____ (in caps) Department _____

Please note that throughout this document, the term 'staff' includes those directly employed by the school, workers from agencies, associate teachers, mentors and volunteers. 'Personal data' and 'Sensitive Personal Data' relates to information/data held about the data subject i.e. the individual student, parent (s) and staff member. 'Private' refers to the individual user signing this agreement.

The ICT user and Confidentiality Agreement at work

The ICT facilities at The Grey Coat Hospital are provided and maintained for the benefit of all, and users must use the facilities responsibly. Other ICT usage rules will be added to the relevant headings when necessary but staff are asked to take advice if unsure about the frequently changing technology and contact options.

The ICT user and Confidentiality Agreement outside the workplace

You should be aware that any use of private communications technology at home or elsewhere, which relates to the school in any way (e.g. school work, emails or texts addressed to other members of the school community, or communications about the school, or about any members of the school community) are subject to this policy. The school name, badge, uniform and motto are the property of the school, and should not be used in any public form of communication on the internet or elsewhere, (e.g. posting on YouTube, Facebook, LinkedIn, internet blogs or any other social networking sites) without the written permission of the headteacher. Please remember that when expressing your personal opinions publicly, you may be perceived as also promoting your professional opinion to those who know your employment type, employment place or status.

Social Media

Staff should ensure their private accounts have the relevant privacy settings and other available security to avoid their accounts being infiltrated or accessed by students, parents or the press. Staff should never accept invitations to join sites initiated by students. These considerations should be applied when using all forms of social media platforms.

General rules on confidentiality, data protection and 'Subject Access'

Students, parents and staff have the right to see their personal information and can make a subject access request to see the personal information the school holds about them. Students and parents also have the right to see their educational records, which includes emails. Personal data of students, parents and staff colleagues must, at all times, be processed in accordance with the rights of data subject under the General Data Protection Regulations. For more information:

<https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation>

Staff working at The Grey Coat Hospital shall not, during their employment at The Grey Coat Hospital or at any time after the employment has terminated, disclose any confidential information (including personal information on students, colleagues, parents or others whose details are or have been kept on computer or

other media) to any unauthorised person or persons or the press. Any such disclosure including information protected by company law will be treated as gross misconduct and render the employee subject to disciplinary action which may result in dismissal. Certain violations may also result in legal action being taken against the ICT user.

Data Breach (source [ICO.org.uk](https://ico.org.uk))

A personal **data breach** is a **breach** of **security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal **data**. If you experience a personal data breach (e.g. loss or theft of a personal device containing work related information, or having your school email hacked) you need to inform the Bursar immediately so that an assessment can be made of the likelihood and severity of the risk to people's rights and freedoms, following the breach. To reduce the risk of a breach:

No personal data of students, staff, parents or visitors may be stored on portable devices.

This includes databases, photos, videos and voice recordings.

Computers, Mobile Equipment and Removable Data Storage

- If absolutely necessary, to keep personal and/or sensitive data outside of SIMS, save on the relevant network drive only. Where personal information needs to be shared electronically please always send on an encrypted email. Discuss with the ICT Manager or Bursar the options to protect or encrypt the data. If you must print information for trips etc. please destroy as soon as it is no longer needed.
- Only use the computers in school, and school devices at home. for educational purposes and make sure you always log off before leaving the computer.
- Do not leave any mobile equipment and/or storage devices unattended which contain any data that is related to the school regardless of its level of confidentiality or the ownership of the equipment. Mobile school devices must be stored securely at all times.
- Devices taken home (once the agreement to do so has been signed) must be stored out of sight in a locked cabinet, in a locked house. Never leave school equipment in a car even when the car is locked. School devices may only be used by the individual who has signed the agreement. Do not leave for others to use. Infringement could result in disciplinary action.
- Always check files brought in on removable media and consult ICT Staff before installing and/or attempting to install or store programs of any type on the computers.
- To protect the ICT systems, damaging, disabling, or otherwise harming or attempting to bypass settings on school computers is prohibited.
- Eating or drinking in the designated computer areas is prohibited.

Electronic Data

- Access to data whether current or archived is provided to those individuals who, in the course of performing their responsibilities and functions, must use the specified data. All data on the network is protected by anti-virus software which runs on servers and workstations, and is updated automatically.
- There are stringent rules about sharing personal data about students, parents and staff and only organisations listed in our data declaration may have access to such information. Please always check with the Bursar before supplying any information to outside bodies or individuals. The school has a legal obligation under the General Data Protection Regulations to hold information on students, parents and staff members in a secure environment. This is also the case for staff information which must not be shared with others without the express written permission of the individual.
- When accessing the files on the school server from outside the school ensure your home computer has anti-virus software installed which must be regularly updated with the latest virus definitions.

- You should not intentionally delete or move a file from any public folder that does not belong to you.
- All electronic resources created by staff when they work at the school, are the property of the school and must be stored in the shared area. Upon employment termination, staff must ask permission from their Head of Department or a member of SLT if they wish to copy any information held of the school network or servers.

Security and Privacy

- Your password must have at least 8 characters, at least one numerical and one capital: remember to change your password regularly and you must not have the same password for SIMs as you have for logging on to the network. Never disclose your username and password to anyone and never use someone else's logon name or password and always log off whenever you have finished using a computer in the school.
- Never leave a computer logged on under your name with SIMS open. SIMS contains all the school data and therefore, it is always essential to log off to ensure Data Protection.
- Never allow a colleague or student to have access to your password, or allow them to use a computer that you have logged in to. Any misdemeanour will be seen as the actions of the individual who has logged on not the third party user.
- ICT staff have access to network storage areas, and individual internet activities are recorded on the server and monitored on a regular basis.

Internet

- You should access the Internet only for school activities. You may access your private emails and other private related websites during non-contact time but school computers should not be used to do so. Do not make non school purchases as the school network may not be secure in that regard. Please note: goods ordered for private use must not be delivered to the school.
- Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school including copyright laws. Staff must not download any electronic copyrighted and/or licensed-required files from any school computer unless the school has the license to do so. Please check before assuming this the case.

Email

- Parents will be advised that communicating by email will not mean they can expect an immediate response.
- Staff choosing to communicate with parents by email must follow school email protocols, see below. The tone of your email should always reflect the ethos of the school. Please remember other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is a disciplinary offence.
- If any individual's name is quoted in an email then they have a right to see it if they ask to do so. Staff must be confident that what is written about an individual is accurate, factual and necessary, and could stand up to a legal challenge.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate nature, report such messages immediately to your line manager and ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden. Offences will be dealt with according to the school's code of conduct.
- Staff must not use their school email address for private communications or to sign up to websites for private use. Staff are advised to tick "do not wish to receive any information from a trusted/selected third party companies".

Email content, etiquette and complying with GDPR

- **School email is not private.** Email correspondence must be included in Subject Access Requests so people can request to see what has been written about them.
- **Addressee.** The people included in the “To” field should be only those that need to read and respond to the message.
- **The ‘CC’ field** should be used only to copy in the people who have a need to know. Use the group options wisely.
- **If selecting ‘reply to all’** consider first if everyone needs to know.
- **Be brief and to the point.** It should be clear at the beginning of the message why you are emailing.
- **Commending and praising** someone is acceptable, but email is not an appropriate medium for criticism. Always think carefully before you report adversely on an individual. Avoid having multiple data subjects in a single message.
- **Choose your words carefully** and be mindful of your tone. The receiver will not have the benefit of your pitch, inflection and other non-verbal cues. Avoid ambiguity and words that might be misinterpreted as the more precise you are the less likely follow up questions seeking clarity will be needed.
- **Do not write in ALL CAPS.** This is the digital equivalent of shouting.
- **Never write or reply in anger.**
- **Re-read your email before you send it!**

Email is not a secure platform. If you would be compromised were your email given to the press, then delete.

I have read and understood the above and agree to use the school ICT equipment and systems within the guidelines outlined above. I accept that I must keep all matters regarding personal data confidential and if I suspect a breach, I will inform the Bursar immediately.

Signature: _____

Name in full: _____

Date: _____