GAYHURST SCHOOL

IT POLICY

THIS POLICY APPLIES TO ALL MEMBERS OF THE SCHOOL COMMUNITY (INCLUDING STAFF & GOVERNORS, LEARNERS, VOLUNTEERS, PARENTS AND CARERS, VISITORS) WHO HAVE ACCESS TO AND ARE USERS OF SCHOOL DIGITAL SYSTEMS, BOTH IN AND OUT OF THE SCHOOL.

P024v14
Reviewed: Autumn 2023
Next Review: Autumn 2024
Compiled by: Head of Computing & Digital Systems

Contents

IT Policy

1. Introduction

Gayhurst School believes that Computing and IT in the 21st Century has the power to make a significant contribution to teaching and learning across all subjects and ages. We believe the school should be at the forefront of new technologies and promote greater awareness and understanding of the role and uses of technology in the modern world.

Technology is increasingly becoming a part of everyday life with computing ubiquitous, so it is vitally important we equip our students for the challenges of tomorrow. To this end we teach them a range of skills which will enable them to interact with the wider world using a range of technological equipment. We also ensure that our students have all the key skills necessary to engage, communicate and interact with the community around them.

We are very aware of the potential problems and issues associated with accessing material available on the internet but see the correct use of internet resources as an essential educational tool in a modern technological society.

Other concerns are the protection of data, security of the network infrastructure, care for the physical equipment, hacking, virus protection and online digital content.

The need for guidelines and rules concerning the use of digital resources at Gayhurst is clearly recognised and, before being allowed to use digital resources, all users must be prepared to accept and abide by AUP (Acceptable Use Policy) rules laid down by the school, see appendices.

2. IT Expectations of Staff

All members of Staff are required to accept an Acceptable Use Policy (AUP) annually prior to login on a school PC located on the Windows network (Appendix) and have a responsibility to use the school’s Internet and email facility in a professional, lawful and ethical manner. The following policy applies to usage from computers whether fixed or portable, or any other computing or telecommunications or data processing device provided or made available by the school or used in the school’s premises.

All staff will be provided with a school-owned device, usually a Microsoft Surface, iPad or iPad mini. Only school issued devices should be used, as this maintains data security. School email may be accessed on a personal mobile, providing no attachments are downloaded directly onto the device.

Staff will be required to enable Multi-Factor Authentication on their Office 365 account (which includes single sign-on), to ensure the integrity of their accounts. This can be done either through the installation of the Microsoft Authenticator app on a mobile device, or through a phone call to a specified number. This will only apply to accounts when accessed off the Gayhurst site.

Staff access the internet through the GH-LAN Wi-Fi network, which is filtered by Smoothwall.

All staff and governors at the school receive annual Online Safety training through the National College CPD website. This gives them an up-to-date knowledge of changes in legislation and current internet safety matters.

Any key information relating to internet safety will be shared as available by the Deputy Head, Director of Digital Learning or the Head of Computing and Digital Systems.

If staff have any concerns whilst browsing online, or whilst using any of the school systems, they should report their concerns to the below, depending on the nature of the concern.

- Safeguarding – DSL or member of the Safeguarding Team
- Technical – IT Support (Concero) or Head of Computing & Digital Systems
- Other – Director of Digital Learning or Head of Computing & Digital Systems

In the case of misuse, the Director of Digital Learning, Head of Computing or IT support staff will inform the Head and provide evidence from the safeguarding filters; or a screenshot taken by the management system. The Deputy Head would then conduct an investigation using the evidence and advise the Head on any relevant actions. In the case of staff, such instances will be dealt with by the Head directly.

3. IT Expectations of Visitors

All visitors are required to accept an Acceptable Use Policy (AUP) when they log on to the school's wireless network and have a responsibility to use the school's Internet facility in a professional, lawful and ethical manner. The following policy applies to usage from computers whether fixed or portable, or any other computing or telecommunications or data processing device provided or made available by the school or used in the school's premises.

Visitors can be provided with the wireless network password if required, by Concero, the Head (or Head's PA), the Bursar, the Deputy Head, Director of Digital Learning or Head of Computing.

Visitors access the internet through the GH-Visitors Wi-Fi network, which is filtered by Smoothwall.

Visitors should not use USB devices when logging into a school device, however, may use them on a personal device if required.

Any key information relating to internet safety will be shared as available by the Head of Computing and Digital Systems.

If visitors have any concerns whilst browsing online, or whilst using any of the school systems, they should report their concerns to the below, depending on the nature of the concern.

- Safeguarding – DSL or Safeguarding Team
- Technical – IT Support (Concero) or Head of Computing & Digital Systems
- Other – Director of Digital Learning or Head of Computing & Digital Systems

In the case of misuse, the Head will be informed and the relevant actions will be taken.

4. Maintaining the Security of the Network

Connection to the Internet significantly increases the risk that a computer or a computer network may be infected by a virus or be accessed by unauthorised persons.

All networked computers and laptops have anti-virus software; this is server managed and automatically scans all files.

As the school uses Office 365 to distribute its mail (and then MS Outlook as a front-end client), Microsoft have anti-virus measures in place to scan all incoming and outgoing e-mails, there is also an email client attached to the firewall for added security.

Despite the above precautions, it is essential for all staff, pupils or visitors do not open e-mail attachments from unknown senders – or if anything looks suspicious. If they are **not sure** then please forward the email to ICT support, who will inform on whether the email is safe.

The school's server is backed up nightly to the cloud, to ensure that we do not suffer losses in case of a breach.

5. Using the Internet

… produces benefits that include:

- Access to a wide variety of educational resources
- Staff Continued Professional Development through access to new curriculum materials, experts' knowledge and practice
- Provision of practical web-based resources to support learning in *every* curriculum area

- Exchange of curriculum and administration data with other teachers and teaching organisations
- Enhanced skills in literacy, particularly in being able to read and appraise critically, and then to communicate what is important to others
- Enhanced research skills in the seeking out, analysis and use of appropriate subject related material
- The ability to facilitate both individual and collaborative learning
- The motivation of having work published on the Web
- Independence in accessing and using a multitude of learning resources
- Confidence from being able to support and extend learning
- Resilience and perseverance whilst searching for relevant information

… enhances learning

Staff and pupils will use the Internet to find and evaluate information. Pupils will, therefore, learn how to use a web browser and older pupils will also be taught searching techniques to locate specific information for themselves. Comparisons will be made between the different sources available for researching information and pupils will learn to decide when it is appropriate to use the Internet as opposed to other sources of information, in terms of: the time taken; the amount of information found; the usefulness, and reliability of information located.

The different ways of accessing information from the Internet will depend on the nature of the material being accessed, and the age of the pupils.

- Access to the Internet may be by teacher demonstration
- Pupils in KS1 will be directed to sites which have been reviewed and selected for content
- Pupils in Lower KS2 may be given tasks to perform using a specific group of websites accessed from the school homepage or their favourites list
- Pupils may be given a specific web page or a single website to access
- Pupils may be provided with lists of relevant and suitable websites which they may access
- Older, more experienced pupils may be allowed to undertake their own Internet search having agreed a search plan with their teacher; pupils will be expected to observe the AUP and will be informed that checks can, and will, be made on files held on the system and the sites they access.
- It is expected that staff test particular search terms they wish their pupils to use prior to lessons as part of their planning and report any inappropriate sites or images to the IT Department.

6. Using E-Mail

Gayhurst uses Office 365. From there, all workstations, including all devices, use MS Outlook (and web-access) as a front-end client. This has the potential for collaborative calendars, task lists, and distribution lists and more through Departments and Key Stages.

Staff have access to Gayhurst Email from portable devices of their own, however are advised that the use of this Email facility is monitored and part of the school domain at all times. Each mobile device can be remotely wiped of school data if and when required.

It is important that communication with persons and organisations are properly managed to ensure appropriate educational use.

Gayhurst advocates the use of the following procedure with regard to viruses.

- The *Know* test

Is the e-mail from someone that you know?

- The *Received* test

Have you received an e-mail from this sender before?

- The *Expect* test

Were you expecting an e-mail with an attachment from this sender?

- The *Sense* test

Does an e-mail from the sender, with the contents as described in the subject line and the name of the attachment(s), make sense?

- The *Virus* test

Does this e-mail contain a virus? Always check it using anti-virus software.

Largely, this procedure is rendered obsolete by anti-virus and anti-spam software: each e-mail is scanned as it enters the school. Vigilance as regards unsolicited e-mails, however, is always a worthwhile course of action.

The school will, periodically, send 'test emails' which will send a mock spam email to all staff and governors. If clicked on, these will require the receiver to complete relevant training to ensure they can identify spam emails.

Please also see the **Staff Code of Conduct** for information regarding the staff use of email.

7. Gayhurst's Website, Portals & SchoolPost

The rationale behind Gayhurst's web presence is to:

- Provide accurate, up-to-date information about the school
- Promote the school
- Inform all stakeholders about calendar events, sports fixtures, links to senior schools, curriculum details and up-to-date news etc.

- Provide resources and links for pupils and parents alike.
- Present data and media for parents to access and interact with
- Act as a communication tool for parents of the school

If a match is cancelled, then this will be communicated by text and email as soon as possible on the day of the fixture. Similarly, in the event of school closure, a pertinent message will appear on the homepage & parents will receive email and text notification.

The following guidelines are observed as far as our web-based content is concerned:

- All classes throughout the school may provide work
- Staff will be responsible for ensuring pupils' work is accurate and the quality of presentation is of a high standard
- The Admissions & Marketing Director are responsible for up-loading pages to the school website, overseeing all content on the website, as well as maintaining and updating the site.
- The Head of Computing & Digital Systems works with all stakeholders to ensure up-to-date information, media and resources are available to parents via the site.

8. Monitoring & Review

The monitoring of the effectiveness of Internet access strategies, and the protection thereof, is the responsibility of the Director of Digital Learning and Concero, with support from the Head of Computing & Digital Systems. All users on the network, however, share a responsibility to adhere to the AUP at all times.

The Director of Digital Learning, in consultation with the rest of the Department, reviews this and appended policies on an annual basis; amendments are made as necessary.

9. Parental support

The school publishes advice on safe internet usage on its website for parents/carers and refers to this on an annual basis. An online E-Safety resource is offered to parents of the school to provide information on how best to support children remaining 'safe online'. Literature is available on the National Online Safety website for the whole parent body.
The school subscribes to National Online Safety for these resources for parents to be able to access a range of advice and support in aiding their child's online usage. This is regularly referred to in Online Safety communication from the school.

10. Prevent Duty

In line with KCSIE September 2021 and the Prevent Duty Guidance effective March 2016, The IT Department monitors internet usage and key search terms, along with the use of the filtering system on a regular basis. Tests are also undertaken with key search terms to ensure access to such terrorist or extremist material is prohibited within the school.

All staff have the responsibility to monitor children in their care and their wellbeing. If there are any concerns on children's desire to access certain material, this should be reported immediately to the school's Designated Safeguarding Lead (DSL).

11. Acceptable Use

11.1. User Actions

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)					X

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	• Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

Consideration should be given for the following activities when undertaken for non-educational purposes:	**Staff and other adults**				**Learners**			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission
Online gaming (not for educational purposes)			X		X			
Online shopping/commerce			X		X			
File sharing (for educational purposes)		X				X		
Social media			X		X			

Messaging/chat using Teams		X			X			
Entertainment streaming e.g. Netflix, Disney+			X		X			
Use of video broadcasting, e.g. YouTube, Teams Live Event				X	X			
Use of personal e-mail in school, or on school network/wi-fi		X			X			
Use of school e-mail for personal e-mails	X				X			

11.2. Acceptable Use Policy (Staff)

Gayhurst expects **you to be responsible for your behaviour on the Internet**, just as you are anywhere else in the school.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.

- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.
- Do not use personal devices, including mobile phones, to download any school information or data.

Compliance with related school policies

You will ensure that you comply with the school's other relevant policies.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Director of Digital Learning. Reports will be treated in confidence.

Acceptance of this policy

Please confirm that you understand and accept this policy. (Accepted on School system)

11.3. Acceptable Use Policy (Visitors)

Gayhurst expects **you to be responsible for your behaviour on the Internet**, just as you are anywhere else in the school.

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems

Whenever you use the school's IT systems (including by connecting your own device to the network) you should follow these principles:

- Only access school IT systems using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Compliance with related school policies

You will ensure that you comply with the school's other relevant policies.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Director of Digital Learning. Reports will be treated in confidence.

Acceptance of this policy

Please confirm that you understand and accept this policy.

Signed: Date:

11.4. Acceptable Use Policy (Pupils in EYFS/KS1)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

Gayhurst expects you to be responsible for your behaviour on the Internet, just as you are anywhere else in the school.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers, iPads, Interactive White Board or other computing equipment
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other computing equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets or worries me on the screen
- I know that if I break the rules, I might not be allowed to use the school's computing equipment.

11.5. Acceptable Use Policy (Pupils in KS2)

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

Gayhurst expects you to be responsible for your behaviour on the Internet, just as you are anywhere else in the school.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the school systems or devices for any on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission
- I understand that, if I do use my own devices in the, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- ¤ Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network/internet and contact with parents.

Sanctions

- Violation of any of the above rules will result in a temporary, or permanent, ban of Internet use.
- Additional disciplinary action may be taken in line with existing school behaviour policies.

12. Rules for Responsible Network Use

The following rules will help to keep you safe & help you to be fair when using the school devices

General Device rules

💻 No food or drink should be consumed anywhere near a school device
💻 Hands should be clean
💻 Take care of screens, keyboards, headphones, mice, monitors & cables
💻 Leave the work area clean & tidy
💻 Keep quiet so that other people can work too

Using the computers

- Use your own username & password to log onto the system
- Do not go into other people’s files
- Do not bring in programs on removable devices & try to install them on the school devices
- Only use the school devices for schoolwork or homework

Printers

- Only print when absolutely necessary
- Always check that your work is finished – check your spelling!
- Only print the required pages
- Choose the correct printer
- Remember to collect your printouts from the printer

Using the Internet

- Ask permission from a teacher before using the Internet
- Always behave in a responsible way
- Report any unpleasant material to a teacher immediately as this will help protect other pupils
- Understand that the school may check computer files & monitor the Internet sites you visit
- Do not give your full name, home address or telephone number to **anyone** over the Internet

You will be held accountable for your actions

13. Guidance for Staff

General guidance for use of internet and social media

- All Staff are expected to use the internet and email facility provided by Gayhurst School in a responsible manner, ensuring they keep the school’s reputation and ethos at mind at all times.

- It is advised that staff remain professional throughout their online activity, including the use of social media sites, such as Facebook, Twitter, Instagram, Snapchat, LinkedIn and any others not listed here.
  All Staff are advised to ensure their privacy settings are appropriately set on social media sites, as well as on personal devices.
- All Staff are advised that they are not permitted to use removable devices such as a USB stick. For guidance regarding this matter, Staff are advised to consult the IT Support Staff.

Please consult the staff code of conduct for more guidance.