



Woodchester Endowed Church of England (Aided) Primary School

‘Love, Learn and Flourish Together’

Our church school community seeks to inspire children and adults to love, learn and flourish together so we may become everything God has created us to be.

Acceptable User Policy

September 2025

Written by:	Lynne Loomes (Headteachers)
Review date:	September 2026
Ratified by Governors:	September 2025

Indeed, the body does not consist of one member but of many’ (1 Corinthians 12; 14-16)

‘Love, Learn and Flourish Together’



Contents

1.	Vision and Rationale	3
2.	Introduction and aims	3
3.	Relevant legislation and guidance	3
4.	Definitions.....	4
5.	Unacceptable use	4
6.	Staff (including governors, volunteers, and contractors)	6
7.	Pupils.....	9
8.	Parents/Carers	12
9.	Data security	12
10.	Protection from cyber attacks.....	14
11.	Internet access.....	15
12.	Monitoring and review	16
13.	Related policies	16
	Appendix 1: Facebook cheat sheet for staff.....	17
	Appendix 2: Acceptable use of the internet: agreement for parents and carers.....	19
	Appendix 3: Acceptable use agreement for older pupils	20
	Appendix 4: Acceptable use agreement for younger pupils	21
	Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors	22
	Appendix 6: Glossary of cyber security terminology	23

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



1. Vision and Rationale

Woodchester Endowed Church of England Primary School community seeks to inspire children and adults to **‘Love, Learn and Flourish Together’** so that we may become everything God has created us to be.

‘Indeed, the body does not consist of one member but of many’ (1 Corinthians 12; 14-16)

As a Church of England school, our Christian vision is central to all we do. Our school community seeks to inspire children and adults to love, learn and flourish together so we may become everything God has created us to be. Our Christian vision is rooted in Paul’s letter to the people of Corinth and in our desire to nurture the whole community, flourishing both now and in the future. Paul reminds them that they should live good lives and that their community will be stronger and make a bigger difference if everyone works together to make the most of their individual talents and skills. Our school vision recognises that we are unique individuals, loved by God, and we aim to develop all children and adults to their full potential through a wide variety of opportunities and experiences.

Woodchester Endowed C of E Primary School is committed to safeguarding and promoting the welfare of all our children and expects all staff, governors and volunteers to share this commitment and behave safely and responsibly when using information and communications technology (ICT). Our systems and curriculum will help educate our children about keeping safe in our ever-changing technological world.

2. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school’s policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use

This policy covers all users of our school’s ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our Code of conduct.

3. Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)
- [Computer Misuse Act 1990](#)

Indeed, the body does not consist of one member but of many’ (1 Corinthians 12; 14-16)

‘Love, Learn and Flourish Together’



- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [Education and Inspections Act 2006](#)
- [Keeping Children Safe in Education 2023](#)
- [Searching, screening and confiscation: advice for schools 2022](#)
- [National Cyber Security Centre \(NCSC\): Cyber Security for Schools](#)
- [Education and Training \(Welfare of Children\) Act 2021](#)
- UK Council for Internet Safety (et al.) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- [Meeting digital and technology standards in schools and colleges](#)
- Keeping children safe in education 2025 <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

4. Definitions

- **“ICT facilities”**: includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service
- **“Users”**: anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **“Personal use”**: any use or activity not directly related to the users’ employment, study or purpose
- **“Authorised personnel”**: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities
- **“Materials”**: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- See appendix 6 for a glossary of cyber security terminology.

5. Unacceptable use

The following is considered unacceptable use of the school’s ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 5.2 below).

Unacceptable use of the school’s ICT facilities includes:

- Using the school’s ICT facilities to breach intellectual property rights or copyright
- Using the school’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school’s policies or procedures

Indeed, the body does not consist of one member but of many’ (1 Corinthians 12; 14-16)

‘Love, Learn and Flourish Together’



- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Using the school's IT equipment or systems to build a personal brand or business
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
 - During assessments, including internal and external assessments, and coursework
 - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

5.1 Exceptions from unacceptable use

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion following a discussion with the headteacher outlining the reasons why use of facilities are required.

- Pupils may use AI tools and generative chatbots:
- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images. All AI-generated content must be properly attributed

5.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies. E.g. Code of Conduct.

Copies of relevant policies are available via the school office, via the staff drive or on the school website.

6. Staff (including governors, volunteers, and contractors)

6.1 Access to school ICT facilities and materials

The school's IT provider/IT Subject Lead/Headteacher manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Headteacher in the first instance.

Use of phones and email

The school provides each member of staff and governor with an email address (firstinitialsurname@woodchester.gloucs.sch.uk).

This email account should be used for work purposes only. Staff should use school laptops where possible to access email. **Where a member of staff is accessing email through a personal device, it is the responsibility of the member of staff to ensure that device is secure at all times.**

All work-related business must be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be password protected so that the information is only accessible by the intended recipient. The Headteacher/SENCO/Office team will use the relevant secure systems that are already in place.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Headteacher and School Business Manager immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in the sections above.

6.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching time.
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the school's ICT facilities to store personal non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities (described below). Where breaches of this policy are found, disciplinary action may be taken.

Staff are not permitted to use their personal devices (such as mobile phones or tablets) unless discussed and agreed with the Headteacher in extenuating circumstances only.

Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain particularly on social media, where pupils and parents could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see above) to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely. They should dial in using a virtual private network (VPN) using school laptops only. Personal devices will not be configured with VPN access into school systems.

The VPN system is managed by GHS who control access to the systems through the use of teacher laptops. VPN access will not be provided outside of school laptops. Staff laptops have inbuilt authentication and security installed which act as a means of securing the hard drive of the laptop. To use VPN staff also need to have their user name and password set up through the VPN gateway via GHS.

If using VPN outside of school, staff must be mindful as to the information being accessed and the environment in which they are situated whilst they access the information. E.g. accessing pupil information in a public place. Staff will ensure that if they are leaving their laptops on they have locked the screen so that information is secure.

If a member of staff requires access to VPN this must be requested via the Headteacher.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the IT supplier may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy. This can be found on the network drive/via the school office or on the school website.

5.4 School social media accounts

The school has an official Facebook page, managed by the Headteacher, which is used to promote school events only. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The school has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities, WiFi and networks. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our governing board is responsible for making sure that:

- The school meets the DfE's [filtering and monitoring standards](#)
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
 - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and ICT manager, as appropriate.

7. Pupils

7.1 Access to ICT facilities

The following ICT facilities are available to pupils:

- Pupil computers and equipment such as pupil iPads and laptops in school are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Pupils will be provided with an account linked to the school's Office 365 instance, which they can access from any device by using their Office365 login. Parents are responsible for ensuring that these are used appropriately when outside of school.

7.2 Search and deletion

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from headteacher/designated safeguarding lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation, proceeding to act according to the behaviour policy if the pupil refuses to co-operate.

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of an inappropriate item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, **and/or**
- Undermine the safe environment of the school or disrupt teaching, **and/or**
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [searching, screening and confiscation](#) and the UK Council for Internet Safety (UKCIS) et al.'s guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)

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

- The DfE's latest guidance on [searching, screening and confiscation](#)
- UKCIS et al.'s guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#)
- The school's behaviour policy.

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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

8. Parents/Carers

8.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course. Parents do however have access to their child's Office365 account. These accounts are provided for educational purposes only and parents/carers may not use their child's Office365 account for any other purpose.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion. This access will be withdrawn when that parent has finished the activity.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

8.2 Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to read the agreement in appendix 2 and notify the school if they are not prepared to abide by this agreement.

8.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out. When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

Parents/carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

9. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

Staff, pupils, parents/carers and others who use the school's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on [digital and technology standards in schools and colleges](#), including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

9.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. GHS manages the password update process for staff.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

GHS will provide passwords for pupils at the start of each school year or upon joining the school. These will be kept in a secure location in case pupils lose or forget their passwords. GHS is able to reset forgotten passwords for pupils and staff.

9.2 Software updates, firewalls and anti-virus software

All of the school's ICT devices that support software updates, security updates and anti-virus products will be configured to perform such updates regularly or automatically by the IT provider.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities including plugging personal devices into school laptops. E.g. hard drives.

Any personal devices using the school's network must all be configured in this way.

9.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy which can be found on the network drive, via the school office or on the school website.

9.4 Access to facilities and materials

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the IT provider.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Headteacher immediately.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

9.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

10. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The school and the IT provider will:

- Work with governors and the school community to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
 - Check the sender address in an email
 - Respond to a request for bank details, personal information or login details
 - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether or IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- The IT provider puts controls in place that are:
 - **Proportionate:** the school will verify this using a third-party audit (such as [360 degree safe](#)) to objectively test that what it has in place is effective
 - **Multi-layered:** everyone will be clear on what to look out for to keep our systems safe
 - **Up-to-date:** with a system in place to monitor when the school needs to update its software
 - **Regularly reviewed and tested:** to make sure the systems are as effective and secure as they can be
- Back up critical data at the relevant frequencies and store these backups securely away from site.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT provider
- Make sure staff:
 - Dial into our network using a virtual private network (VPN) when working from home
 - Enable multi-factor authentication where they can, on things like school email accounts
 - Store passwords securely
- Make sure the ICT provider conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the [Cyber Essentials](#) certification
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify [Action Fraud](#) of the incident. This plan will be reviewed and tested at least annually or after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'
- Work with our local authority to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

11. Internet access

The school wireless internet connection is secured which is:

- Filtered using Securely software provided by GHS
- Used by all approved users (staff/pupils/governors/parents)

Should an inappropriate website be accessible through the filter then the Teacher is responsible for notifying the Headteacher and then raising a call with the IT provider to update the filter. Should a site be filtered by accident, then the Teacher is responsible for raising a call with the IT provider to have the website added to the safe list.

The software will send an alert to the Headteacher with the details of any inappropriate website and the time it was accessed. If it has been accessed by a Windows user, the alert will contain details of the user. If it is an iPad user the alert will not contain details of the user and the Headteacher will speak with all class teachers to ascertain the details.

10.1 Parents and visitors

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher. The school has a visitor WiFi and can provide login details as required.

The headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Staff must not give the school Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

12. Monitoring and review

The headteacher, IT subject lead and IT provider will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The governing body is responsible for approving this policy.

13. Related policies

This policy should be read alongside the school's policies on:

- Child protection and safeguarding
- Code of Conduct - Staff
- Data protection

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

Recommendations for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider reviewing Facebook app security settings on your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to '**Friends only**', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've '**liked**', even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



What to do if...

A pupil or parent adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil or parent asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils or parents and that if they persist, you'll have to notify senior leadership. If the pupil or parent persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the headteacher about what's happening

A parent/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the school
 - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material

If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Appendix 2: Acceptable use of the internet: agreement for parents and carers

Please note that unless parents/carers contact the school it is expected that all will agree to the terms of the agreement below.

Parents/carers also set up channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, or chats (through apps such as WhatsApp), however these are independent of school.

Acceptable use of the internet: agreement for parents and carers

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Our official Facebook page
- Email/text groups for parents (for school announcements and information)
- Class DoJo
- Tapestry Learning Journal
- Pupil Office365 instance including Teams

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's social media, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the school's social media, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Appendix 3: Acceptable use agreement for older pupils

Teachers will review these conditions with children as part of online safety teaching at the start of lessons.

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
 - During assessments, including internal and external assessments, and coursework
 - To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Appendix 4: Acceptable use agreement for younger pupils

Teachers will review these conditions with children as part of online safety teaching at the start of lessons.

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- Share my password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard, to create images or write for me, and then submit it as my own work

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

It is expected that all will accept these conditions unless discussed with the headteacher. The headteacher reserves the right to withdraw access to the school's ICT facilities should staff/governors/volunteers or visitors not accept these conditions.

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



Appendix 6: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'



TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.

Indeed, the body does not consist of one member but of many' (1 Corinthians 12; 14-16)

'Love, Learn and Flourish Together'

