

ICT, internet acceptable use policy and social media

Woodfield School

Combined policy



Approved by:	Full Governing Board	Date: 18/05/2026
Last reviewed on:	May 2026	
Next review due by:	May 2027	

Contents

1. Introduction and aims	2
2. Relevant legislation and guidance	3
3. Definitions	3
4. Unacceptable use of ICT, Social Media and Online Platforms.....	4
5. Staff (including governors, volunteers, and contractors)	5
6. Pupils.....	9
7. Parents/carers.....	10
8. Data security	10
9. Protection from cyber attacks.....	12
10. Internet access	13
11. Monitoring and review	13
12. Related policies	14
13. Breach of This Policy	14
Appendix 1: Acceptable use of the internet: agreement for parents and carers.....	15
Appendix 2: Acceptable user agreement for pupils and parents/carers.	15
Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors	18
Appendix 4: Glossary of cyber security terminology	19

1. 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 the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses could 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/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Preventing disruption that could occur 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
- enable appropriate use of social networking sites in a safe and secure manner
- safeguard employees in their use of social networking sites and ensure they do not make themselves vulnerable
- minimise the risks to us through use of social media.

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, visitors, agency workers and anyone who has access to our IT and communication systems. This policy does not form part of any employee's contract of employment, and it may be amended at any time. We may also vary this policy as appropriate in any case.

Misuse of IT and communications systems can damage our school and our reputation. Breaches of this policy may be dealt with under our disciplinary policy.

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, 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](#)
- › [Data \(Use and Access\) Act 2025](#)
- › [Computer Misuse Act 1990](#)
- › [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 2025](#)
- › [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](#)
- › [Meeting digital and technology standards in schools and colleges](#)

3. Definitions

- › **ICT facilities:** 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 that may become available in the future which is provided as part of the school's ICT service
- › **Users:** anyone authorised by the school to use the school's 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 agreed by an authorised user
- › **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 school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- › **Social media:** is the term used for internet-enabled tools used on computers, tablets, smart phones and other smart devices etc to allow people to share information, ideas and views.

See appendix 5 for a glossary of cyber security terminology.

4. Unacceptable use of ICT, social media and Online Platforms

The following is considered unacceptable use of the school's ICT facilities, systems, devices, internet access, social media platforms or online communication tools. Any breach of this policy may result in disciplinary action and, where appropriate, referral to external agencies.

Unacceptable use includes:

- Using ICT systems, social media or online platforms in a way that is unlawful, unsafe, discriminatory, abusive, threatening, intimidating, obscene or offensive
- Bullying, harassment, victimisation or promoting unlawful discrimination, including racist, homophobic, antisemitic, extremist or radicalised content
- Using inappropriate, offensive or profane language, gestures, images, videos, audio or other content, including explicit lyrics or sexually explicit material
- Accessing, creating, storing, sharing or distributing pornographic, obscene, harmful or otherwise inappropriate content, including nude or semi-nude images, videos or livestreams
- Making, endorsing, liking, reposting, sharing or commenting on content that is defamatory, derogatory, speculative or could bring the school, its staff, pupils or wider community into disrepute
- Making false, misleading or malicious statements about the school or members of the school community
- Sharing confidential, sensitive or personal information relating to the school, pupils, parents/carers or staff in breach of confidentiality, safeguarding expectations or data protection legislation
- Impersonating another individual or misrepresenting views as those of the school without authorisation
- Creating social media accounts, posts or communications on behalf of the school, or using the school's name, logo or branding without prior authorisation
- Using professional school email addresses for personal social media or networking accounts
- Using the school's ICT systems for unauthorised personal business, advertising, gambling, phishing, scams or financial gain
- Participating in online chat rooms, blogs, forums or messaging platforms in a manner that breaches school expectations or professional standards
- Connecting unauthorised devices, software, applications or web services to the school's ICT systems or network
- Attempting to gain unauthorised access to systems, accounts, restricted areas, password-protected information or data
- Allowing others to gain unauthorised access to school systems, accounts or information
- Circumventing the school's filtering, monitoring or security systems
- Causing deliberate damage to ICT systems, networks, equipment, software or data
- Removing, altering, deleting or sharing school information or data without authorisation
- Causing or contributing to a data breach through unauthorised access, sharing or misuse of information
- Breaching intellectual property rights, copyright or licensing agreements
- Engaging in conduct online that compromises professional boundaries, safeguarding responsibilities or the reputation of the school
- Providing references, endorsements or statements on behalf of the school without express authorisation from the Headteacher

The examples above include creating, posting, sharing, forwarding, reacting to, endorsing, liking, commenting on or distributing any text, images, videos, audio recordings, livestreams or other online content through websites, social media platforms, messaging applications or digital communication systems.

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

4.1 Exceptions from unacceptable use

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.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on Staff Disciplinary and staff code of conduct.

You can find a copy of our schools disciplinary policy on the One Drive, under All Staff – [Staff Disciplinary Policy](#).

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

5.1 Access to school ICT facilities and materials

The school's ICT lead manages 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 login/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the ICT lead and member of SLT for permission to access these files.

5.1.1 Use of school-supplied equipment

School-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the school. All school-supplied equipment remains the property of the school and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for school purposes and in line with the school's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from school. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. Passwords must:
 - Not be shared with others and must be changed regularly
 - Be suitably strong, in accordance with the school's password policy (see section [8.1])
 - Not be reused across multiple accounts

- › Update software, operating systems and applications when prompted, or as directed by the ICT lead
- › Connect to the school network using approved and secure methods. When connecting to wi-fi networks outside of the school, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- › Report any loss, theft, damage or compromise of a school device promptly to the ICT lead, designated safeguarding lead and data protection officer

5.1.2 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff must make sure multi-factor authentication is enabled on their email account(s).

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

Staff must not share their personal email addresses with parents/carers 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 subject access requests from individuals under the UK GDPR and 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.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted using a strong, state-of-the-art encryption standard so that the information is only accessible by the intended recipient.

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 ICT lead, immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the phones provided by the school to conduct all work-related business.

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 section 4.

5.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The ICT lead/SLT may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- › Does not take place during contracted hours/teaching hours/non-break 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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as tablets) in line with the school's ICT policy.

Staff may not store any school-related data on personal devices, on cloud storage or on personal removable storage devices.

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, where pupils and parents/carers could see them.

Staff are expected to adhere to the school's guidance regarding the use of social media, as set out within this policy. The school's social media expectations and requirements are incorporated into this combined ICT and Acceptable Use Policy and use of email (see section 5.1.2) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should make sure their use of social media, either for work or personal purposes, is always appropriate.

All social media platforms, including, but not limited to:

Twitter, Facebook, Instagram, LinkedIn, YouTube, TikTok and message boards are included as part of this policy.

It also includes any website where you can contribute or edit content and instant messaging services i.e., WhatsApp, Snapchat etc.

This policy also applies to any other existing or new social media platform not mentioned, whether internal or external or used on a personal or work device.

All forms of social media use are covered by this policy, this can include but is not limited to; posting comments, pictures or videos, blogging, using forums, sending private messages, endorsing other people's content, re-tweeting/circulating posts or adding/editing content on a website.

If it can be determined from your account that you work for us (either visually, verbally or written), we ask that you make it clear that any content and views are your own. Confirming this point does not make you exempt from following this policy.

Please include "these views are my own and not that of my employer" on your profile.

You should make it clear in social media postings that you are speaking on your own behalf.

You should be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see. You should ensure that you use privacy and access settings whilst being aware that you cannot control the use of your postings by others.

You should also ensure any content you post on social media are consistent with the professional image you present to colleagues, pupils, and parents.

If you are uncertain or concerned about the appropriateness of any statement or posting, you are advised to refrain from posting it until they have discussed it with their line manager.

If you become aware of social media content that disparages or reflects poorly on us, you should contact your line manager or Headteacher.

5.3 Use of emojis, GIF's and Memes

Using emojis, GIF's or Memes do have their benefits, however it is important to use them correctly and appropriately.

You should be aware that messages and comments that include emojis may affect the way text is read. Emojis may mean different things to different people, the use of them may mean the text is deemed inappropriate.

If you chose to use emojis, GIF's or Memes you should ensure they are appropriate and easily understood within the

context.

5.4 Remote access

We allow staff to access the school's ICT facilities and materials remotely.

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 must take such precautions as the ICT Lead /SBM may require 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, which can be found [here](#).

5.5 Absence from Work and use of Social Media

Use of social media whilst absent can create the impression that staff are well enough to be working. We accept that this is not necessarily the case, but this may be how it is perceived by colleagues and others. Taking this into account we would guide staff to be mindful of their use of social media during absence from work.

5.6 School social media accounts

The school has an official Facebook account, managed by ICT lead. 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 may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.7 Monitoring and filtering of the school network and use of ICT facilities

To comply with Department for Education (DfE) guidance on [meeting digital and technology standards](#), and to safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

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

We reserve the right to monitor, intercept and review your use of social media. We consider valid reasons for checking your internet usage include suspicions that you have:

- been using social media when you should have been working.
- acted in a way that is in breach of the rules set out in this policy.

Monitoring is in our legitimate interests and is to ensure that this policy is being complied with.

For further information, please refer to data security policy.

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

The school reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the school, including for the following purposes.

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

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.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the 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

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, in line with our behaviour/discipline 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 making 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 or 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
- › Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- › Causing intentional damage to the school's ICT facilities or materials
- › Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- › Using inappropriate or offensive language

7. Parents/carers

7.1 Access to ICT facilities and materials

Parents/carers do not have access to the school's ICT facilities as a matter of course.

However, parents/carers 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.

Where parents/carers are granted access in this way, they must abide by this policy.

7.2 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/carers 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/carers to sign the agreement in appendix 1.

7.3 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.

8. 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 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

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. Users must not use the same passwords across multiple platforms.

All passwords should have at least one special character, number and capital letter in them.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.

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

All staff will use the password manager required by the ICT lead to help them store their passwords securely.

When temporary passwords are allocated by the ICT lead these must be disposed of securely once used.

8.2 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 have these installed, and be configured to perform such updates regularly or automatically.

Users should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from Damien Hart (ICT Lead).

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.

Any incoming files should always be virus-checked by the ICT department before they are downloaded.

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

8.3 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 [here](#).

8.4 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 ICT lead/SLT

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 ICT lead immediately.

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 shut down completely at the end of each working day.

8.5 Encryption

The school makes sure 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, as defined by the ICT lead.

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for all users, including staff, pupils and governors (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:
 - The methods hackers use for tricking people into disclosing personal information, including phishing
 - Online safety and password security
 - Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
 - The physical security of devices, for example not leaving a laptop unlocked and unattended
 - The risks of using removable storage media, such as USBs
 - Multi-factor authentication
 - How and when to report a cyber incident or attack
 - How and when to report a data breach
 - Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training

Please note: the list of training content above is also included in our online safety model policy – you don't need to include it in both policies, so delete the list from here if you also include it in another school policy

- How to check the sender address in an email
- How to respond to a request for bank details, personal information or login details
- How to 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 our 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
- Put controls in place that are:
 - **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 – Daily, Weekly, Monthly and Quarterly on two separate onsite backups.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department.
- 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 using a password manager
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)
- Make sure effective cyber breach prevention measures and processes are in place, e.g. endpoint detection and response systems
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the [Cyber Essentials](#) (or a similarly effective and recognised) 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 annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'
- Work with our LA to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement
- Conduct a cyber risk assessment at least annually, and revisit it every term, or after a significant event has occurred
- Appoint a digital lead (from the senior leadership team) to oversee cyber risk assessment

10. Internet access

The school's wireless internet connection is secure.

10.1 Parents/carers and visitors

Parents/carers and visitors to the school will only be permitted to use the school's guest WiFi as granted by the headteacher.

The headteacher will only grant authorisation if:

- Parents/carers 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 WiFi 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)

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

11. Monitoring and review

The headteacher and ICT Lead 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 board is responsible for Reviewing and approving this policy.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education
- Artificial Intelligence (AI)

13. Breach of This Policy

Breach of this policy may result in disciplinary action up to and including dismissal.

You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

Where this policy requires you to disclose matters from your personal life, we will consider the circumstances and context of each matter before determining whether any further action is required.

Appendix 1: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
Name of parent/carer:	
Name of child:	
<p>Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels:</p> <ul style="list-style-type: none">• Email/text groups for parents (for school announcements and information)• Arbor <p>Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).</p>	
<p>When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:</p> <ul style="list-style-type: none">• 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 <p>I will not:</p> <ul style="list-style-type: none">• Use private groups, the school's Facebook page, 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 unless they are raised in an appropriate way• Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a school-related 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 the other children's parents/carers	
Signed:	Date:

Appendix 2: Acceptable user agreement for pupils and parents/carers.

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

Name of pupil:

At our school, we use computers, tablets, the internet and other technology to help pupils learn, communicate and stay safe.

Staff will support pupils to use technology safely and appropriately at all times.

When using school technology and the internet, pupils are expected to:

- Use technology safely and kindly
- Follow instructions from school staff
- Use technology for learning and school activities
- Be respectful to others online
- Tell a trusted adult if they see or hear something upsetting, unsafe or worrying
- Keep personal information safe
- Use school devices and equipment carefully

Pupils must not:

- Use technology without staff permission or supervision
- Visit unsafe or inappropriate websites
- Use social media, chat rooms or messaging apps unless this is part of a planned learning activity supervised by staff
- Use rude, hurtful or inappropriate language, images or videos
- Bully, upset or be unkind to others online
- Share personal information or passwords
- Pretend to be someone else online
- Take, send or share inappropriate photos, videos or livestreams, including images where someone is not fully clothed
- Damage school equipment or use technology in a way that is unsafe

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.

The school may respond to unsafe or inappropriate online behaviour in line with the Behaviour Policy, Safeguarding Policy and ICT Acceptable Use Policy.

Signed (pupil):

Date:

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.

Signed (parent/carer):

Date:

Appendix 3: Acceptable use agreement for staff, governors, volunteers and visitors

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

Name of staff member/governor/volunteer/visitor:

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 any illegal or 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 any private business, 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.

Signed (staff member/governor/volunteer/visitor):

Date:

Appendix 4: 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. Many of these terms are from the National Cyber Security Centre (NCSC) [glossary](#).

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure 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	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised 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 who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses with the end aim of fixing them.

TERM	DEFINITION
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 or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
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	Programmes 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 people in an organisation.