Wincheap Foundation Primary School

ICT and Internet Acceptable Use Policy

Ratified by	Learning and Teaching Committee
Date of Approval	10th November 2026
Authors	Network Manager
Responsible Committee / Board	Finances & Premises Committee
Review Date	1st November 2027
Target Audience	Staff/Governors/Parents/Visitors

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 2
3. Definitions 3
4. Unacceptable use 4
5. Staff (including governors, volunteers, and contractors) 5
6. Pupils 8
7. Parents/carers 10
8. Data security 11
9. Protection from cyber attacks 12
10. Internet access 13
11. Monitoring and review 13
Appendix 1: Acceptable use agreement for staff, governors, volunteers and visitors 14
Appendix 2: Glossary of cyber security terminology 16

---

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
- Prevent 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

This policy applies to all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors. In certain cases—such as when generative AI is used to complete homework—it also applies to non-school ICT devices where, for example, they are used to produce material for school work or bringing the school into disrepute on social media. Breaches of this policy may be dealt with under Wincheap's relevant discipline and conduct policies.

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regards 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

This policy should be read in conjunction with other relevant school policies, including:

- Online safety
- Safeguarding and Child Protection
- Behaviour
- Staff discipline
- Parental Code of Conduct
- Data Protection and GDPR
- Cybersecurity
- Mobile Phones
- Artificial Intelligence (AI)

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

See appendix 6 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 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
- 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 illegal, inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- 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 the Network Manager, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's 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 the Network Manager or Headteacher
- 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
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from the Network Manager or Headteacher
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school and permitted by the Headteacher
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Using AI tools and generative chatbots (such as ChatGPT or Google Bard):
    - During assessments, including internal and external assessments, and coursework

- To write homework or 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 or anyone delegated by her will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of ICT.

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.

Staff and pupils may use AI tools and generative chatbots as research aids to explore new topics and ideas. However, they must present their findings in their own words. Any AI-generated content included in their work must be clearly marked as such and be a small percentage of the whole. The main aim of any written piece in these situations is to allow the writer to explore their own thoughts and develop their own clarity of communication. The over-use of AI can undermine this.

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 relevant discipline and conduct policies.

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

5.1 Access to school ICT facilities and materials

The school's Network Manager oversees and regulates 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 find they 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 Network Manager.

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 Network Manager
- 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 Network Manager and to the Headteacher.

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 should enable multi-factor authentication 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 own 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 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.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted 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 Network Manager 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 Headteacher may withdraw or restrict this permission at any time and at her discretion.

Personal use is permitted provided that such use:

- Does not take place during any period where staff are expected to be working
- Does not constitute 'unacceptable use', as defined in section 4, above
- 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 mobile phones or tablets) in line with the school's policies.

Staff may not store any school-related data on personal devices, on personal 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 should take care to follow the school's guidelines on use of social media and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity or bringing the school into disrepute.

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 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 a very small number of 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 Network Manager 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 and cybersecurity policies.
.

5.4 School social media accounts

The school has official Facebook and Instagram accounts, managed by the Headteacher and Network Manager. 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.

5.5 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

Only authorised ICT personnel or services 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 body, via the Headteacher, 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 Accessing ICT facilities

School computers and ICT equipment are available to pupils only under the supervision of staff

Unless express permission is granted by the Headteacher, pupils should not bring in mobile phones, tablets, smart watches or any other personal ICT devices. These items are banned because any device that is capable of recording images or sound or accessing the internet without adult supervision contravenes the school's Online Safety and Data

Protection and GDPR policy. Where permission has been granted by the Headteacher, all devices must be handed in at the School Office upon arrival at school.

6.2 Search and deletion

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 an illegal or 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:

- Abusive, illegal or inappropriate messages, images or videos
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Note: Mere suspicion that a pupil possesses a banned device is not, by itself, sufficient grounds for a personal search. Staff must have reasonable grounds to suspect that the device has been used in a way that breaches the law or poses a serious risk under school policies before conducting a search.

Staff conducting searches must comply with the school's Positive Handling policy and Mobile Phones policy and the DfE's latest guidance on searching, screening and confiscation

Staff members should:

- Inform a member of the SLT or a DSL of any incidents where they had reasonable grounds to suspect a pupil is in possession of a banned item and a search may be necessary.
- ask for the suspicious item to be handed to them, but **should not** conduct a search themselves unless they have been specifically authorised to do so by the Headteacher.
- Involve the Headteacher or a DSL 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 staff member to decide on a suitable response. Depending on the seriousness, they should consider if the Headteacher or a member of SLT needs to become involved. 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 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, they will:

- Not view the image
- Not copy, print, share, store or save the image
- Confiscate the device and report the incident to the Headteacher or a DSL immediately, who will decide what to do next.

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 take appropriate action, in line with the relevant school policies, 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 illegal, offensive or 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 Friends of Wincheap School) 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 to abide by the Code of Conduct (Parents/Visitors) which can be found on the school website.

7.3 Communicating with parents/carers about pupil activity

We ask parents/carers to supervise their child's online activities to ensure they are safe and using the internet acceptably.

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. Please contact your child's teacher in the first instance.

8. Data security

In conformity with our Cybersecurity, Online Safety and Data Protection&GDPR policies, 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.

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, visitors or volunteers who disclose account or password information may have their access rights revoked.

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 the Network Manager.

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 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 the school's Data Protection and GDPR policy.

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 the Network Manager.

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 Network Manager immediately.

In accordance with the Clean Desk Clear Screen policy, 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 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 Network Manager.

9. Protection from cyber attacks

Please see the glossary (appendix 2) 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 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.
- 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:
  - **Proportionate**: the school will verify this using a third-party audit (such as 360 degree safe) [insert frequency – at least annually], 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 and store these backups on cloud-based backup systems/external hard drives that aren't connected to the school network and which can be stored off the school premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider selected by the Network Manager
- Make sure staff:
  - Use appropriate, strong security when accessing the school network from home
  - Enable multi-factor authentication where they can, on things like school email accounts
  - Store passwords securely, preferably using a password manager
  - Remain vigilant against attempts to access school devices and/or systems by the use of malware or phishing links within emails. Even if it is from someone known to the staff member, if something feels wrong, seek advice from the Network Manager before clicking on the link or opening the attachment.

This list is not exhaustive. Please refer to the Cybersecurity policy for more detailed systems and expectations to protect and respond to cyber attacks.

10. Internet access

The school's wireless internet connection is secure and filters are in place to ensure internet use is safe and appropriate. However, in an ever-evolving online environment the systems and procedures can never be one hundred percent foolproof so adults must be vigilant in their vetting and supervising of online sources and immediately report to the Network Manager any websites or links that connect to unsafe or inappropriate material.

10.1 Pupils

Pupils do not have unsupervised access to the internet via the school's computers and ICT equipment and should never need access to the school WiFi access codes as personal devices are not permitted.

10.2 Parents/carers and visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation in rare situations, such as:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the Friends of Wincheap School)
- 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)

Where the WiFi access is authorised by the Headteacher, ideally the code should be inputted by a member of staff so that it cannot be shared further.

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 Network Manager 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 annually by the Learning and Teaching committee of the governing body.

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 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.

If I choose to use my own ICT facilities when working outside school, I will follow the Acceptable Use Policy while doing so.

I will let the designated safeguarding lead (DSL) 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 2: 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.

term	definition
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.
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.