WILLIAM FARR

C of E Comprehensive School

ICT and Internet Acceptable Use Policy

Contents

0. Vision and Values

William Farr (C of E) Comprehensive School's vision is to provide all members of the school community with the opportunities to engage with 'life in all its fullness' (John 10:10) through the highest quality of education, encouragement and endeavour. We are committed to striving for excellence and ensuring that all students are known, valued and can achieve.

Our core values are: Compassion; Friendship; Perseverance; Respect; Responsibility; Wisdom.

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 students, 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, students, 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 students safe and effective internet and ICT use.

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

Breaches of this policy may be dealt with under our (student) behaviour policy or staff discipline policy.

2. 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
- 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

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, students, 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 5 for a glossary of cyber security terminology.

4. Unacceptable use

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 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
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its students, 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 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 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
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel

- 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
- 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
- Inappropriate use of AI tools and generative chatbots (such as ChatGPT and Google Bard) to generate text or imagery presented as original work.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher or other relevant member of the SLT 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

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that is not listed above and may be considered an unacceptable use, permission for such usage may be granted at the headteacher's or appropriate member of SLT's discretion.

Use of AI tools and generative chatbots as a research tool may be permissible provided any AI-generated content is properly attributed.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies on (student) behaviour and staff discipline.

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

5.1 Access to school ICT facilities and materials

The school's ICT manager 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 manager in the first instance, although authorisation may need approval from the relevant member of SLT.

5.1.1 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 personal email addresses with parents/carers and students, 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 ICT manager and member of SLT responsible for GDPR immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or students. Staff must use 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.

The school can record incoming and outgoing phone conversations. This is stated on each call made into school and is for training and monitoring purposes.

Staff who would access a recorded phone conversation should speak to the ICT manager and complete the school's request form.

Requests that would typically be approved include:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents/carers to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs (SEN) assessments, etc.
- Discussing requests for term-time holidays.

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

It is recommended that staff avoid using 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 there are limits on their storage and backup. Use of the school's ICT facilities for personal use may also 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) to access the school network and their 365 account. They should have appropriate and up-to-date security and access the system via Microsoft authenticator.

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 students and parents/carers could see them.

Staff should take care to follow the school's guidelines on use of email (see section 5.1.1) and be aware of the recommendations regarding use of social media from this policy (see Appendix 4) 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 appropriate at all times.

5.3 Remote access

We allow staff to access the school's ICT facilities and materials remotely via Office 365. Staff also have limited access to the school network via the quick links section of the school website.

We allow students limited access to the school network via remote access. Information on remote access can be found under the student section on the school website.

Where possible dial in should be using a virtual private network (VPN).

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 school 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.

5.4 School social media accounts

The school has official social media accounts, overseen by the ICT staff or those given permission to manage individual accounts by the headteacher of relevant member of the SLT. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

Those who are authorised to manage, or post to, the account must make sure that the material they post or link to is appropriate for students and is in keeping with the ethos of the school at all times.

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

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 and Safeguarding personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. Information is provided to parents about the school systems via the school website.

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. Students

6.1 Access to ICT facilities

Computers and equipment in the school's ICT suites are available to students under the supervision of staff. Computers in the Resources area are available to students with the permission of the library staff.

Students may also use departmental laptops in lessons whilst SEN students can book out laptops from the SEN department for use in lessons.

All students are expected to use their ICT access for educational purposes only in line with the student code of conduct.

Sixth Form students can use the computers in school independently for educational purposes only.

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 students 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 students, **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 students and staff. If the search is not urgent, they will seek advice from the headteacher, designated safeguarding lead or other appropriate member of SLT
- Explain to the student 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 student's co-operation (or apply the school behaviour policy should a student refuse to cooperate)

The authorised staff member should:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a student was in possession of a banned 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 staff member in conjunction with the DSL, headteacher or other member of the senior leadership team 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 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 student 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 students 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
- Our behaviour policy
- Any complaints about searching for, or deleting, inappropriate images or files on students' 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 students, in line with the behaviour policy, where there has been misuse of the ICT accounts and access provided by the school. Similarly, the school will sanction for any misuse of ICT equipment provided by the school. This is **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 students, 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 as it applies to staff.

7.2 Communicating with or about the school online

We believe it is important to model for students, 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 2.

7.3 Communicating with parents/carers about student activity

Parents and carers must expect that students will be permitted to use a variety of online resources for educational purposes including the internet for research.

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, students, 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 suitably strong passwords for their accounts and keep these passwords secure.

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 students 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.

Staff may use password managers (eg Microsoft Edge) to help them store their passwords securely. ICT staff will generate passwords for students using the required password manager or generator and keep these in a secure location in case students lose or forget their passwords.

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 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 data protection regulations and the school's data protection 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 ICT 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 ICT manager 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 use personal devices (including computers and USB drives) to access school data and work remotely if the devices have appropriate levels of security.

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 ICT department 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 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 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 daily (automatically) and store these backups on Barracuda (cloud-based backup)
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to Bromcom
- Make sure staff:
    - Dial into our network using the remote server 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
- 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 checking 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 annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box' or equivalent.

10. Internet access

The school's wireless internet connection is secure. There is a filtering system in place (WatchGuard) and different Wifi connections for staff/students/visitors.

10.1 Students

The school's wireless connection is available throughout the school and students can access via a login to the student wifi connection. The filtering system and additional protections ensure that students can access no more than they could via the school network.

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 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, the appropriate member of SLT and the ICT 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 every three years.

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

Policies can be found on the school website under Policies or on the VLE under Governors > Policies.

Appendix 1: KS3, KS4 and KS5 acceptable use agreement (Network Code of Conduct (student and parents/carers) [Pre-Sept 24]

WILLIAM FARR

C of E Comprehensive School

Agreed Information Technology Code of Conduct for using the Network, Internet and e-mail at school.

Please read the following points carefully and make sure that you understand everything before signing the consent form. Students granted access to the school network, including e-mail, will abide by the IT Code of Conduct.
All users of the Network and Internet are expected to abide by these rules of computer and network use.

- Be polite when using e-mail. Do not use e-mail to bully or insult others.
- Do not use inappropriate or unacceptable language.
- Never reveal your personal address or telephone number or those of fellow students to people unknown to you.
- e-mail is monitored by the school security system. Never say anything or engage in anything that you would not be happy to write on a postcard that could be read by everyone.
- Inform a member of staff IMMEDIATELY you discover an obscene or offensive web page so that its access can be blocked.

Students agree that they will **NOT PERFORM** the following unacceptable actions:

- Try to bypass the internet security.
- Complete questionnaires or subscription forms without checking with a member of staff.
- Damage, degrade or disrupt the performance of equipment or systems.
- Attempt to retrieve information about 'hacking' or attempt to 'hack' our system.
- Download programmes.
- Play computer games unless they have permission from their teacher to play subject based games / learning activities as part of the curriculum.
- Send or display offending messages, pictures, videos or sound.
- Use the internet to buy or sell anything.
- Use the internet to access obscene or offensive web pages/material.
- Use the network for any illegal activity, including the violation of copyright or other laws.
- Use someone else's account, either with or without permission.
- Waste printer paper.
- Tell another student your password.

The school will electronically audit your Internet and e-mail usage at all times and a record of this is kept.

Student and parent/guardian consent:
No student will be granted access to the Internet without both student and parent/guardian signing the Code of Conduct consent form.

The consent form allows parents/guardians to confirm that their child may or may not have access to the Internet.

The consent form confirms that the student has read and agrees to abide by the Code of Conduct.

Agreed Information Technology Code of Conduct for using the Network, Internet and e-mail at school

Student Name: _____

Form _____

Username if known: _____

Student Consent Form

I have read and agree to abide by the IT Code of Conduct in both letter and ethos. I understand that breaching the Code will result in the sanctions by the school.

Student signature: _____

Parent/Guardian Consent Form

I understand that my child now has the opportunity to have access to the Internet and an e-mail address. I have read the school's IT Code of Conduct and *grant/do not grant my permission for my child to have access to the Internet and e-mail.

Signed: _____

Date: _____

Print Name: _____

*Delete as appropriate

Appendix 2: KS3, KS4 and KS5 acceptable use agreement (students and parents/carers) [Sept 2024 onward]

WILLIAM FARR

C of E Comprehensive School

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Name of student:	**Form:**

When I use the school's ICT systems and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only observing copyright and other laws
- Only use them when a member of staff is present, or has given permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a member of staff immediately if I find any material which might upset, distress or harm me or others
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless a member of staff has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, or download programmes without first checking with a member of staff
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate
- Attempt to 'hack' the school's IT systems or bypass its monitoring and security systems
- Damage, degrade or disrupt the performance of equipment or IT systems
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

If I bring a personal electronic device into school:

- I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission
- I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online

I understand that the school will monitor my use of the school network, email and the internet and that records will be kept as appropriate.

I agree to abide by this code of conduct and understand that there will be consequences if I don't follow the rules.

Signed (student):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STUDENTS AND PARENTS/CARERS	
Parent/carer's agreement: I understand that my child can use the school's ICT systems, email and internet. I agree to the conditions set out above for students 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 (staff, governors, volunteers and visitors) [2024 onward]

WILLIAM FARR
C of E Comprehensive School

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, FRIENDS OF THE SCHOOL, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 • Take photographs of students without checking with teachers first • Share confidential information about the school, its students 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 will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree 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 student 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 students in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Social Media Guidance for staff

The following guidance has been collated for staff from The Key.

Do not accept friend requests from pupils on social media

10 recommendations for school staff on Social Media

1. Check your privacy settings regularly
2. Don't share anything publicly that you wouldn't be happy showing your students
3. Be careful about tagging other staff members in images or posts
4. Don't make comments about your job, your colleagues, our school or your students online – once it's out there, it's out there
5. 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)
6. 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
7. Consider the display name you use on sites such as Facebook – you could use your first and middle name, use a maiden name, or put your surname backwards instead
8. Consider your profile pictures – make sure that the image is professional. You could change your profile picture to something unidentifiable
9. Be aware that apps such as Facebook recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or students)
10. Avoid using social media sites during school hours.

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, students 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.

What to do if …

A student adds you on social media

- In the first instance, ignore and delete the request. Block the student from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the student asks you about the friend request in person, tell them that you're not allowed to accept friend requests from students and that if they persist, you'll have to notify senior leadership and/or their parents/carers. If the student 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
    - Students 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 student or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer 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.

Appendix 5: 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.
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 (such as bank

TERM	DEFINITION
	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	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.