BLESSED HUGH FARINGDON CATHOLIC SCHOOL

ICT AND ACCEPTABLE USE POLICY

All that happens in Blessed Hugh Faringdon Catholic School occurs within the context of the school's Mission Statement (in accordance with the Trust Deed for the maintenance and advancement of the Catholic religion).

Written: January 2026
Updated:
Adopted: January 2026
Persons Responsible: Headteacher
Committee: Full Governing Body
Review Due: Annually – January 2027

As a Catholic school, founded on, and committed to upholding the teaching of the Church, we believe that Jesus is present in the day-to-day life of our community and that each member of our community has a divine origin and an eternal destiny. In discharging our responsibilities, we are guided by the principles of Catholic social teaching [CST], in which the following core values are constituted: dignity, solidarity, the common good, the option for the poor, the promotion of peace, care for creation, the dignity of work and the value of participation in society. These principles are demonstrated in our core, and wider, curriculum, in our care of students, in our work with the disadvantaged and in the outward-facing approach to our local community, our nation and to the world. As our moral compass, CST guides us in all our school activities, including the formulation, upholding and reviewing of school policies.

As a Catholic school, we regard the following characteristics as central to the human flourishing of everyone – students, staff and Governors – in our community. Our aspirations for our students are that their experience of teaching develops in them a lived belief, an authentic sense of true happiness, a lived sense of family, an experience of care and a vocation for service.

To achieve these aspirations, teaching and learning will privilege the following core virtues for every member of our community.
Grateful for their own gifts, for the gift of other people, and for the blessings of each day; and generous with their gifts, becoming men and women for others.
Attentive to their experience and to their vocation; and discerning about the choices they make and the effects of those choices.
Compassionate towards others, near and far, especially the less fortunate; and loving by their just actions and forgiving words.
Faith-filled in their beliefs and hopeful for the future.
Eloquent and truthful in what they say of themselves, the relations between people, and the world.
Learned, finding God in all things; and wise in the ways they use their learning for the common good.
Curious about everything; and active in their engagement with the world, changing what they can for the better.
Intentional in the way they live and use the resources of the earth, guided by conscience; and prophetic in the example they set to others.

Contents

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

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 Staff Code of Conduct, Disciplinary Policy and Procedures or Behaviour for Learning 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 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 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
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard):
    - During assessments, including internal and external assessments, and coursework
    - To write their homework or class assignments, where AI-generated text or imagery is presented as their own work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher, DSL or other suitable SLT member, nominated by 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. A representation must be made to the Headteacher clearly explaining the reasons. The Headteacher may involve the DSL or Head of Operations who line manages IT Support in such decisions.

Students may use AI tools and generative chatbots:

- As a research tool to help them find out about new topics and ideas
- When specifically studying and discussing AI in schoolwork, for example in ICT lessons or art homework about AI-generated images. All AI-generated content must be 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 following school's policies:

- Staff Code of Conduct
- Disciplinary Policy and Procedures
- Behaviour for Learning Policy

Students and staff misusing the system will engage in discussions to develop their understanding of appropriate use and sanctions will be issued as appropriate.

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

5.1 Access to school ICT facilities and materials

The school's IT 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 should contact IT Support (cc the Head of Operations). The Head of Operations will refer to the DSL if the files are of a Safeguarding nature.

Staff who need their access permissions updated or changed, should contact IT Support in the first instance. The request will be dealt with as required or referred to the DSL for advice if access to Safeguarding systems is being requested.

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.

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 Data Protection Officer (Head of Operations) 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 and Teams meetings. Recordings may be made for training, monitoring or to ensure accurate records.

Ad-hoc recordings may be made by staff. Automatic audio and visual alerts may be made when recording begins. If staff are recording with external participants, they must begin the recording and then further advise the external participant that the recording has begun, giving them the option to end the session if they do not consent.

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 school 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 working hours
- 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

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 Mobile Phone Protocol and Staff Code of Conduct. This includes reference to staff not taking photos of students from a personal device.

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 social media (see Staff Code of Conduct) and use of email (see section 5.1.1) 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.

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

5.3 Remote access

We allow staff to access the school’s ICT facilities and materials remotely from their school laptop, mobile phone and other personally owned equipment.

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 an official Facebook and Instagram account, managed by the Headteacher. The Assistant Headteacher with responsibility for the sixth form manages @bhfcs6thform on Instagram and the PE Department. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, these accounts.

Any other department or area wishing to establish a school-based social media platform should request permission from the Headteacher.

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 Filtering and Monitoring of the school network and use of ICT facilities

The DSL has overall responsibility for Filtering and Monitoring as required by the DfE. 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 may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The school monitors ICT use in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal requirement. This is not an exhaustive list. The school reserves the right to amend this list at any time.

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

Staff and students have the following access:

- Computers and equipment in the school's ICT suites are available to students 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
- Students will be provided with an account, which they can access from any device
- "Sixth-form students can use the computers in the study rooms 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 (see Searching, Screening and Confiscation Policy) can search students and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting as follows. (Staff work in pairs and both staff members must be of the same sex as the student being searched):

- 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 (see Searching, Screening and Confiscation Policy), **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 members are satisfied that they have reasonable grounds for suspecting any of the above, they will follow the guidance in the Searching, Screening and Confiscation Policy including:

- 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, DSL or Deputy Headteacher.
- Explaining 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
- Seeking the student's co-operation and follow guidance in the Searching, Screening and Confiscation Policy where this is not forthcoming.

The authorised staff members 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. A list of banned items is available in our Searching, Screening and Confiscation Policy and the accompanying A4 Searching, Screening and Confiscation Arrangements posted in key staff offices.
- Involve the DSL (or DDSL) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members (DSL, named SLT and the DDSLs) 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 members 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 DSL / Headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

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

practicable. If the material is not suspected to be evidence in relation to an offence DSL/ Headteacher will advise on deletion 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 DDSL) 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
- Any complaints about searching for, or deleting, inappropriate images or files on students' devices will be dealt with through the school Complaints Policy and Procedures.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction students, in line with the Behaviour for Learning Policy if a student 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 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.

Should parents/carers be 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 for adults 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 or about the school through our website and social media channels. Our expectations are outlined in our Visitors on Site Policy.

7.3 Communicating with parents/carers about student 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 students 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 students 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, 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 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.

All staff will use the password manager required by the IT Manager to help them store their passwords securely. Teachers 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 IT Support.

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 IT Support or the Head of Operations (Data Protection Officer) 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 student 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 IT Manager.

9. Protection from cyber attacks

Please see the glossary (appendix 6) 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 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 verify this as part of the process of checking our filtering and monitoring systems and guidance, provided by IT Support, on how to respond to potential suspect emails.
- **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 regularly and store these backups on a cloud-based backup system.

Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider

- Make sure staff:
  - 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
- 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

10. Wi-Fi access on personal devices

The school's wireless internet connection is secure.

When connecting personal devices users should be aware that content accessed may be subject to the same recording monitoring and filtering as on school managed devices.

10.1 Staff

Staff may access Wi-Fi on their personal devices throughout the school.

The school's bring your own device Wi-Fi must be used for this purpose. Staff may only join their own personally owned devices to this network and must use their own school account. Staff must not join school devices or devices owned by others to this network.

Filtering on this network, for staff, is limited. Staff should be mindful about the content they access while in school considering the rest of this policy and other relevant policies.

10.2 Students

Sixth form students, only, may access Wi-Fi on their personal devices throughout the school.

The school's bring your own device Wi-Fi must be used for this purpose. Students may only join their own personally owned devices to this network and must use their own school account. Students must not join school devices or devices owned by others to this network.

The school makes every effort to filter the content available on this network. Students must not attempt to bypass the filtering, for example by using a VPN or other software or programs.

Students should be mindful that the school's ability to filter content on their personal devices is more limited than on school owned devices and be mindful about the content they access.

Students in Key Stage 3 and 4 do not have access to school's bring your own device Wi-Fi.

10.3 Parents/carers and visitors

Parents/carers and visitors to the school may be permitted to use the school's Wi-Fi and, if so, must follow the sign in procedure on arrival and a code will be generated.

11. Monitoring and review

The Headteacher, DSL, Head of Operations (DPO) and IT 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.

The governing board is responsible for approving this policy.

12. Related policies

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

- Online safety
- Child Protection and Safeguarding
- Behaviour for Learning
- Staff Disciplinary Policy and Procedures
- Data protection
- Mobile phone Policy
- Searching, Screening and Confiscation Policy
- Use of Artificial Intelligence Policy
- Marking Protocol
- Visitors on Site Policy

Appendix 1: Facebook Guidance for Staff

Do not accept friend requests from pupils on social media

10 rules for school staff on Facebook

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

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
- Ensure you 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 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. 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.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	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.