Title	**ICT and internet acceptable use policy**
Purpose	Sets guidelines and rules around acceptable use of ICT and internet for all members of our Multi-Academy Trust community
Relevant to	Trustees, Local Governors, all staff, students, parents
Responsible Officer	Business Director, BSET
Introduced	7/2019
Modification History	7/2021, 7/2023, 7/2025
Related Policies	Behaviour; Staff Discipline; Safeguarding; Data Protection
Date Due for Review	7/2027
Relevant committee for review	Board of Trustees
Approved	21 July 2025
Filed as	BSET_Pol.28_ICT_Acceptable_Use_Vs3.1_0725

Contents

1. INTRODUCTION AND AIMS 2

2. RELEVANT LEGISLATION AND GUIDANCE 4

3. DEFINITIONS 4

4. UNACCEPTABLE USE 5

5. STAFF (INCLUDING GOVERNORS, VOLUNTEERS, AND CONTRACTORS) 6

6. STUDENTS 10

7. PARENTS 12

8. DATA SECURITY 13

9. PROTECTION FROM CYBER ATTACKS 14

10 INTERNET ACCESS 15

11. MONITORING AND REVIEW 16

12. RELATED POLICIES 16

APPENDIX 1: FACEBOOK GUIDANCE FOR STAFF 17

APPENDIX 2: ACCEPTABLE USE STANDARDS FOR STUDENTS 19

APPENDIX 3: ACCEPTABLE USE STANDARDS FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS 20

APPENDIX 4: GLOSSARY OF CYBER SECURITY TERMINOLOGY 21

1. Introduction and aims

ICT is an integral part of the way that our schools and provisions work, and is a critical resource for students, staff, governors, trustees, volunteers and visitors. It supports teaching and learning, as well as pastoral and administrative functions of the Academy Trust.

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

This policy is adopted from a model document published by "The Key" and aims to:

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

This policy covers all users of ICT facilities, including trustees, governors, staff, students, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under relevant behaviour or staff disciplinary policies maintained by the school or Academy Trust.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- 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
- The 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

This policy also complies with Barnet Special Education Trust's master and supplemental funding agreements.

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the school to use the ICT facilities, including governors, staff, students, volunteers, contractors and visitors

"Personal use": any use or activity not directly related to the users' employment, study or purpose

"Authorised personnel": employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities

"Materials": files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of ICT facilities by any member of the Academy Trust community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of ICT facilities includes:

- Using ICT facilities to breach intellectual property rights or copyright
- Using ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the school or Academy Trust, or risks bringing the school or Academy Trust into disrepute
- Unauthorised sharing of confidential information about a school, its students, or other members of the Academy Trust community
- Connecting any device to a school's ICT network without prior approval from authorised personnel
- Setting up any software, applications or web services on a school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to a school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school or Academy Trust
- Using websites or mechanisms to bypass a school's filtering mechanisms

This list is not exhaustive. The Academy Trust reserves the right to amend this list at any time. The relevant headteacher or relevant member of Senior Leadership Team will use professional judgement

to determine whether any act or behaviour not on the list above is considered unacceptable use of ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of Academy Trust ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may only be granted at a headteacher's discretion.

Any user of Academy Trust ICT services who believes they may require exceptional permissions, should consult their line manager, so that the case can be properly considered by school leaders following relevant technical, safeguarding, data protection or other legal advice.

4.2 Sanctions

Students and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with Behaviour or Staff Discipline policies.

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

5.1 Access to school ICT facilities and materials

The Academy Trust's IT team manages access to each school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain online services, programmes or files

Permanently employed staff will be provided with unique log-in/account information and passwords that they must use when accessing ICT facilities.

At a headteacher's discretion, accounts may also be provided for temporary members of staff who are agency contractors.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Team via the online helpdesk.

5.1.1 Use of phones and email

The Academy Trust provides each permanent member of staff with an email address.

At a headteacher's discretion, email accounts may also be provided for temporary members of staff who are agency contractors.

This email account should be used for work purposes only.

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

Staff must not share their personal email addresses with parents 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 which contains the personal information of another person, they must inform the designated data protection lead (currently the Academy Development Director) immediately and follow school data breach procedure.

Staff must not give their personal phone numbers to parents 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.

5.2 Personal use

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

Personal use is permitted provided that such use:

- Does not take place during contact time/non-break 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

Staff may not use the Academy Trust 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 Academy Trust ICT facilities for personal use may put personal communications within the scope of a school's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with Staff Handbook guidance

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 could see them.

Staff should take care to follow the school's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal Devices

Staff may only use approved personally owned devices to access the school network as necessary in the course of their normal work (See 8.5). However, the widespread use of cloud-based services for email and document applications means that more work may be safely undertaken on employees' own personal devices (smartphone, tablet, laptop). This will be permitted as long as the device adheres to a strong password and security policy.

Users are forbidden from copying sensitive data from cloud-based email, calendar and contact applications from their work accounts to other storage applications on a personal device.

Staff using personal devices to access cloud-based IT services in relation to their work will be subject to all standards of acceptable use outlined across this document.

Staff agree to a general code of conduct that recognises the need to protect confidential data that is stored on, or accessed using, a personal mobile device. This includes but is not limited to:

- Doing what is necessary to ensure the adequate physical security of the device
- Maintaining and keeping up-to-date the device's operating systems, software configuration and installed applications to ensure the latest digital security measures are applied.
- Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes or security setting changes
- Preventing the storage of sensitive company data on the device.
- Immediately reporting a lost or stolen device.

Support needs or issues related to personal smartphone and tablet devices remain the responsibility of the device owner.

Barnet Special Education Trust and Oak Lodge School will accept no responsibility for loss or damage to any personal device.

5.2.2 Personal social media accounts

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

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

5.3 Remote access

We allow staff to access Academy Trust ICT facilities and materials remotely. This is managed as a supplementary service of London Grid for Learning; use of which requires additional software to be installed on a school computer and a secondary security device.

Remote access facilities will only be granted to Academy Trust owned equipment. Staff may request remote access arrangements through the IT Manager.

Staff accessing Academy Trust 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 ICT facilities outside the school and take such precautions as the IT Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

A copy of the Academy Trust Data Protection Policy is available at www.bsentrust.org.

5.4 Social media accounts

A school or other provision may choose to operate an official social media account, managed by the Headteacher. Staff members who have not been authorised by the Headteacher to manage, or post to, the account, must not access, or attempt to access, the account.

Any school who operates an official social media account will establish guidelines for what may and must not be posted on its social media account. Those who are authorised to manage, or post to, the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of school networks and use of ICT facilities

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Academy Trust reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

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

The Academy Trust monitors ICT use in order to:

- Obtain information related to Academy Trust business
- Investigate compliance with Academy Trust policies, procedures and standards
- Ensure effective Academy Trust 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 Academy Trust board is responsible for making sure that:

- The Academy Trust 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 teams 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 monitoring and filtering systems

Each 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 a school's DSL and ICT manager, as appropriate.

6. Students

6.1 Access to ICT facilities

- Unless designated for specific personal use (such as a communication aid), computers and other forms of ICT equipment 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.
- "Where appropriate and according to their needs and abilities, students will be provided with a limited function account linked to a school's network, which they will be able to access under staff supervision.

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 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 and/or designated safeguarding lead
- 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
- 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 DSL and/or 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, 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

6.3 Unacceptable use of ICT and the internet outside of school

A school may sanction students, in line with the behaviour 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 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
- 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 ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

A school will contact relevant external agencies where it is suspected or believed that an unlawful action has been undertaken, or where wider safeguarding concerns may arise from breaches of our acceptable use policy.

7. Parents

7.1 Access to ICT facilities and materials

Parents/carers do not have access to our 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) 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, where they are used.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask 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, 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 a 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 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 our school's ICT devices that support software updates, security updates, and anti-virus products will 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 a school's network must also 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.

A copy of the Academy Trust Data Protection Policy is available at www.bsentrust.org.

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 Facilities 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 Facilities 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 closed down completely at the end of each working day.

8.5 Encryption

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

School staff may only use personal devices (including computers and USB drives) to access school network 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.

For further policy on use of personal devices refer to section 5.2.1

9. Protection from cyber attacks

Please see the glossary (appendix 4) 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 using a third-party audit 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 daily and store these backups on cloud based systems
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud based supplier
- 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
- Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our suppliers to see what they can further offer the school regarding cyber security.

10 Internet access

Each school's wireless internet connection is secured and filtering software monitoring is in force for all school users.

There is a separate wireless network available for guests or non-school devices. Parents and visitors to the school will not generally be permitted to use the school's Wi-Fi access unless specific authorisation is granted by the headteacher.

The headteacher will only grant authorisation if:

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

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

11. Monitoring and review

The Business Director and IT Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the Academy Trust.

This policy will be reviewed every 2 years.

The governing board is responsible for approval of this policy.

12. Related policies

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

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: Facebook Guidance for Staff

Don't accept friend requests from students 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 not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your 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
- 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 do to 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. 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 adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
    - Responding to one parent'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'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 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 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: Acceptable Use Standards for Students

When a student uses the school's ICT facilities (like computers and equipment) and get on the internet in school, they do not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share a password with others or log in using someone else's name or password
- Bully other people
- Use artificial intelligence (AI) chatbots, such as ChatGPT or Google Bard Google Gemini, to create images or write for me, and then submit it as my own work

Students should understand that the school will check the websites they visit and how they use the school's computers and equipment. This is so that they can be helped to keep safe.

Students must tell a teacher or other member of staff immediately if they find anything on a school computer or online that upsets them, or that they know is mean or wrong.

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

Students should understand that the school can intervene if they do certain unacceptable things online, even if they are not in school when they do them.

Appendix 3: Acceptable Use Standards for Staff, Governors, Volunteers and Visitors

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

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its 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 understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

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

I will let the designated safeguarding lead (DSL) and Facilities 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.

Appendix 4: Glossary of cyber security terminology

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.