ICT and Internet Acceptable Use Policy

Date drafted	**January 2023**
Date approved by Trustees	**February 2023**
Date to be reviewed	**February 2026**

Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 4
4. Unacceptable use 4
5. Users (including staff, trustees, governors, other volunteers, and contractors/ temps/ supply staff) 6
6. Pupils 10
7. Parents 14
8. Data security 14
9. Protection from cyber attacks 16
10. Internet access 17
11. Monitoring and review 17
12. Related policies 18
Appendix 1: Facebook cheat sheet for staff 19
Appendix 2: Acceptable use agreement for staff, governors, volunteers and visitors 22
Appendix 3: Glossary of cyber security terminology 23

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Trust works, and is a critical resource for pupils, staff, trustees, governors, other volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the Trust.

However, the ICT resources and facilities our Trust uses could also pose risks to data protection, online safety and safeguarding if not suitable manged and used.

This policy aims to:

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

This policy covers all users of Trust ICT facilities, including trustees, governors, other volunteers, staff, pupils, contractors/ temps/ supply staff and visitors.

Breaches of this policy may be dealt with under the applicable disciplinary or, behaviour 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 2022
- 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
- UKCIS 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 which may become available in the future which is provided as part of the Trust's ICT service
- **Users:** anyone authorised by the Trust to use the Trust's ICT facilities, including trustees, members, governors, other volunteers, staff, pupils, contractors/ temps/ supply staff 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 Trust to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the Trust'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 Trust's ICT facilities. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching a Trust or school specific policy or procedure
- 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 Trust or any of its schools, or risks bringing the same into disrepute
- Sharing confidential information about the Trust, its schools, its pupils, or other members of the Trust community
- Connecting any device to the Trust's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust'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 Trust'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 Trust's ICT facilities
- Causing intentional damage to the Trust's ICT facilities
- Removing, deleting or disposing of the Trust'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 Trust and this has been appropriately authorised

- Using websites or mechanisms to bypass the Trust's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

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

4.1 Exceptions from unacceptable use

Where the use of Trust ICT facilities (on 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 discretion of the Head Teacher, Chief Executive Officer or Chief Operating Officer in consultation with the Head of IT and specific documented approval must be sought. It is anticipated such instances will be extremely rare.

4.2 Sanctions

Pupils, staff and other users who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust and or School's policy on behaviour as applicable. All current policies can be found on the Trust and individual school websites and the Trust's Staff Portal.

Additionally, the Trust reserves the right to apply ICT use specific sanctions in the interest of cyber and data security (for instance, revoking permission to use the Trust's system(s)).

5. Users (including staff, trustees, governors, other volunteers, and contractors/ temps/ supply staff)

5.1 Access to Trust ICT facilities and materials

Each school's IT Manager manages access to the Trust's ICT facilities and materials for staff and other users in line with the agreed access needs set by the Trust. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programmes or files

Users will be provided with unique login/account information and passwords that they must use when accessing the Trust's ICT facilities.

Users 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 relevant IT Manager.

A request to access additional information will need to be approved by the Head Teacher (CEO or COO in the case of the Central Team) depending on the information that is being requested access to.

5.1.1 Use of phones and email

The Trust provides each member of staff with an account which includes online storage and email facilities.

This account should be used for work purposes only. Users will be expected to enable multi-factor authentication on their account(s) when requested to do so by the Trust, which is in the process of rolling this out to all users, beginning with priority groups.

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

Users must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.

Users 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.

Users 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 users 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 a user sends an email in error that contains the personal information of another person, they must inform the Trust's Data Protection Officer and seek assistance from the IT Team immediately and follow our data breach procedure.

Users must not give their personal phone number(s) to parents or pupils. Users must use any phones provided by the Trust (fixed line or mobile as applicable to the role) to conduct all work-related business.

Trust phones must not be used for personal matters.

Users 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 Trust has the facility to record incoming and outgoing phone conversations on the fixed line system and reserves the right to do so in line data protection legislation.

Users who would like to record a phone conversation should speak to their IT Manager to configure this setting on the phone system.

All non-standard recordings of phone conversations must be approved in advance and consent obtained from all parties involved.

The Data Protection Officer may grant requests to record conversations when:

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

5.2 Personal use

Users are permitted to occasionally use Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The relevant IT Manager or Senior Manager may withdraw or restrict this permission at any time and at their discretion if such use conflicts with the interests of the Trust.

Personal use is permitted provided that such use:

- Does not take place during the working hours of the user
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their job/ role, or prevent other users or pupils from using the facilities for work or educational purposes

Users may not use the Trust's ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Users should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Users are also permitted to use their personal devices (such as mobile phones or tablets) on the Trust network in line with the relevant school's BYOD (bring your own device) policy.

Users should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils, parents and members of the public could see them.

Users should take care to follow the Trust's guidelines on use of 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 social media accounts

Members of staff, trustees, governors and members should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

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

5.3 Remote access

The Trust allows relevant users to access the Trust's ICT facilities and materials remotely. This access is granted via Office 365, which is accessible externally.

The Trust makes use of a remote desktop web client as a method of accessing a small number of systems. The remote desktop web client is maintained by the Trust and is routinely updated.

Users accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Users must be particularly vigilant if they use the Trust's ICT facilities off-site and take such precautions as the Trust 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 at all times, not excluding when being accessed remotely.

5.4 School social media accounts

The Trust has a number of official Twitter and LinkedIn accounts, managed by the Marketing & Communications Officer. Staff members who have not been authorised to manage, or post to, the accounts, must not access, or attempt to access, the accounts.

Serious breaches of the Trust's Acceptable Usage Policy, including any mis-use of social media which either does or could bring the name of the Trust into disrepute may be considered as Gross Misconduct under the Trust's Disciplinary policy.

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

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Trust 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
- Application use

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

The effectiveness of the Trust's filtering and monitoring will be regularly reviewed.

Where appropriate, authorised personnel will raise concerns about monitored activity with the relevant school's Designated Safeguarding Lead (DSL).

The Trust monitors ICT use in order to:

- Safeguard our pupils
- Obtain information related to Trust business and school activities
- Investigate compliance with 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

The Trust Board will regularly review the effectiveness of the monitoring and filtering systems.

6. Pupils

6.1 Access to ICT facilities

Pupils will have access to ICT facilities as follows:

- Computers and equipment in the school's ICT suite(s) will be available to pupils. This will be under the supervision of staff in most cases, but schools can choose to designate specific locations and times where facilities may be accessible to pupils unsupervised.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff.
- Pupils will be provided with an account on the Trust's Office 365 platform.
- All student use should be for educational purposes.

6.2 Search and deletion

Under the Education Act 2011, the Head Teacher, and any member of staff authorised to do so by the Head Teacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as 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 pupils and staff. If the search is not urgent, they will seek advice from the Head Teacher / Designated Safeguarding Lead as appropriate
- Explain to the pupil 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 pupil's co-operation (if the pupil refuses to co-operate, the staff member will proceed according to the school's behaviour policy)

The authorised staff member will:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil 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, 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 / Head Teacher as appropriate 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 if there is a good reason to erase data or files from a device, staff members will consider if 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 reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**

- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (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) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The relevant school behaviour policy
- Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the complaints procedure.

6.3 Unacceptable use of ICT and the internet by pupils outside of school

Trust schools will sanction pupils, in line with their behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust or 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 Trust, or risks bringing the school or Trust into disrepute
- Sharing confidential information about the school or Trust, other pupils, or other members of the Trust 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 Trust's ICT facilities
- Causing intentional damage to the Trust'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

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the Trust in an official capacity (for instance, as a volunteer or as a member of PTA or similar) may be granted an appropriate level of access or be permitted to use the Trust's facilities in this capacity.

Where parents are granted access in this way, they must abide by this policy as a user.

7.2 Communicating with or about the Trust online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with their child's school through our websites and social media channels.

We ask parents to sign the Acceptable Use Agreement when their child joins the school.

7.3 Communicating with parents about pupil activity

We will only communicate with parents regarding pupil ICT use if that activity is in breach of this policy.

Parents may seek any support and advice from the school to ensure a safe online environment is established for their child.

8. Data security

The Trust 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 threat technologies.

Staff, pupils, parents and others who use the Trust's ICT facilities should use safe computing practices at all times. We structure our ICT arrangements 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 Trust's ICT facilities are required set complex passwords for their accounts and keep these passwords secure. We enforce password requirements on the Trust Network that follow the Guidance from the NCSC.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff, or pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers (including members, trustees and governors) who disclose account or password information may have their access rights revoked and there ongoing role re-evaluated.

Passwords are allocated to users when they join the Trust. On first logon they will be required to change their password to one of their own choosing in line with the complexity requirements set in the system.

8.2 Software updates, firewalls and anti-virus software

All of the Trust'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 Trust's ICT facilities.

Any personal devices using the Trust's network/ systems must also be configured in this way. This means that staff will be expected to ensure that their mobile device or personal computer are kept up to date in line with manufacturers' guidelines.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy, this can be found in the Staff Portal and on the Trust website.

8.4 Access to facilities and materials

All users of the Trust's ICT facilities will have clearly defined access rights to systems, files and devices.

These access rights are managed by relevant IT Team, under the direction of the Trust's Head of IT.

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 IT Team and Data Protection Officer immediately.

Users must always log out of systems and or lock their equipment when 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 by users.

8.5 Encryption

The Trust makes sure that its devices and systems have an appropriate level of encryption. In particular all staff laptops and similar devices are encrypted and no Trust owned computer will allow data to be written to an unencrypted external drive or device.

Use of external storage devices with Trust equipment requires them to be encrypted to be able to have information stored on them, should be used only as a last resort and with the support and assistance of the relevant IT Team.

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The Trust will:

- Work with all relevant members of the Trust community to make sure cyber security is given the time and resources it needs to make the Trust and its schools as secure as possible
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the annual training window) on the basics of cyber security, based on the current NCSC guidance.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure.
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data.
- Put controls in place that are:
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up to date:** with a system in place to monitor when the Trust needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Back up critical data and store these backups on removable media, to ensure safety and security.
- Make sure staff:
    - Connect into our network using the approved methods when working from home
    - Enable multi-factor authentication where they can
    - Store passwords securely using a password manager or into a browser that has been signed in with their Trust Account

- Make sure IT staff conduct regular access reviews to make sure each user in the Trust has the right level of permissions and admin rights

- Have a firewall in place that is switched on

- Maintain and test an incident response plan including, for example, how we will communicate with everyone if usual communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed annually and after any significant event/ change has occurred, using the NCSC's 'Exercise in a Box' .

10. Internet access

The Trust's wireless internet provision is appropriately secured, and it subdivided into networks that allow specific groups of users (pupils, staff, guests have their own distinct Wi-Fi networks) or devices (BYOD, Staff Managed Devices) access to only the appropriate areas of the network or internet they require.

10.1 Pupils

Each Trust school is equipped with Wi-Fi coverage to all areas and this is made available to pupils in line with the school specific usage policy.

The Wi-Fi network is filtered in line with the Trust's standard internet filtering policy. Refer to Section 5.5 above

10.2 Parents and visitors

Parents and visitors to Trust schools will not be permitted to use the Trust's WiFi unless specific authorisation has been granted.

The authorisation will only grant authorisation if:

- Parents are working with the school/ Trust in an official capacity (e.g. as a volunteer or as a member of the PTA or similar)

- Visitors need to access the Trust'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)

These Visitors will be given access to a Guest Wi-Fi network only and this will be restricted from accessing the main network.

11. Monitoring and review

The Head of IT is responsible for monitoring the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust.

This policy will be reviewed every three years or when a significant event or change occurs impacting the policy.

12. Related policies

This policy should be read alongside the Trust's (and where appropriate school specific) policies on:

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education
- Mobile device usage

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for pupil-facing 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, 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 pupils
6. Don't use social media sites during school/ working hours
7. Don't make comments about your job, your colleagues, our Trust or schools or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the Trust or our schools 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 pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils 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 pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the Senior Leadership Team or the Head Teacher 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 others at the school
    - Pupils 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 pupil or member of the Trust community, our management and disciplinary procedures should be used 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 agreement for staff, governors, volunteers and visitors

Acceptable use of the Trust's ICT facilities and the internet: agreement for staff, trustees, governors, other volunteers, contractors/ temps/ supply staff and visitors

Name:

When using the Trust's ICT facilities and accessing the internet on-site, or off-site on a work device or on Trust business on another 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 Trsut's reputation
- 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 Trust's network
- Share my password with others or log in to the Trust's network using someone else's details
- Share confidential information about the Trust, any of its school, its pupils, staff, or other members of the Trust community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote a private businesses, unless that business is directly related to the Trust and I have explicit permission to do so.
- Connect any personal device to Trust ICT facilities (on site or remotely) which is not up to date with current security updates as specified by the manufacturer and within its support life.

I understand that the Trust will monitor the websites I visit and my use of the Trust'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 Trust's data protection policy.

I will let the Designated Safeguarding Lead (DSL) and IT Manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the Trust's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed :	**Date:**

Appendix 3: Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber-attack and the measures the Trust will put in place. They are 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.

TERM	DEFINITION
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 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 two or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.

TERM	DEFINITION
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.