CHILTERN LEARNING TRUST

School ICT Internet and Social Media acceptable use policy

[Insert school name]

Date Reviewed	Body	Next Review Date

Summer Term 2025	Board of Trustees	Summer Term 2026

Contents

1. 3
2. 3
3. 4
4. 4
5. 6
6. 10
7. 11
8. 12
9. 12
10. 13

Appendix 1: Personal use of all social media platforms, including management of privacy settings 14

Appendix 2: Glossary of cyber security terminology 16

Appendix 3: Acceptable use of the internet: agreement for parents and carers 17

1. Introduction and Aims

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

Likewise, Social Media is used by our school for communication, networking, and sharing information. It allows us to connect with parents, carers, current and future staff, the wider education sector, other stakeholders and the communities we serve.

However, the ICT resources and facilities and the social media our staff uses could also pose risks to data protection, online safety and safeguarding.

The School understands that many people may choose to use social media sites/applications in their private lives. This policy does not seek to prevent the personal use of social media sites/applications, but does also seek to provide clear guidelines on the acceptable use of all social media by employees for work or in their private lives.

This policy aims to:

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

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

Breaches of this policy may be dealt with under the Trust's Code of Conduct.

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 2024
- DfE Political impartiality in schools guidance

- 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 7settings working with children and young people
- Meeting digital and technology standards in schools and colleges
- The Data Use and Access Act 2025
- DfE's product safety expectations for AI tools

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 any of our school's ICT service or those provided for the Central Team
- **Users:** anyone authorised by a school or the Trust to use our ICT facilities, including governors, staff, volunteers, contractors and visitors
- **Personal:** 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 or Trust to perform systems administration and/or monitoring of the ICT facilities
- **Materials:** files and data created using the Trust's or a school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs
- **Social Media:** any online platform or any application that allows parties to communicate instantly with each other or to share data in a public forum

See Appendix 2 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the school's ICT facilities or social media. Any breach of this policy may result in disciplinary or behaviour proceedings.

Unacceptable use of the school's ICT facilities includes:

- Using the ICT facilities to breach intellectual property rights or copyright (all users should be aware that student work remains the intellectual property of the student and therefore uploading student work to an AI system that learns from its inputs eg. for marking, could constitute a breach of intellectual copyright).
- Using the 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 Trust or our school, or risks bringing the school or Trust into disrepute
- Sharing confidential information about the Trust, our school, our pupils, or other members of the Trust and 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 Trust or our 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 Google Gemini) unless approved following consultation with the Trust's EdTech lead and following a Data Processing Impact Assessment (DPIA), there is also a list of Trust approved tool maintained,

Unacceptable use of Social Media includes:

- Disclosing private and/or confidential information relating to pupils, parents, other Trust employees, their employment directly, or the Trust. This also applies to any other educational establishment that the employee has worked within.
- Discussing or revealing any matters relating to our school or to the Trust, previous educational establishments, Trust employees, pupils or parents.
- Publishing, sharing, distributing or commenting on any material that may be deemed contrary to British Values.
- Publishing, sharing, distributing or commenting on any material that may be deemed contrary to the Trust's legal duty to remain politically impartial
- Identifying themselves as a representative of our school or the Trust online, or on their social media sites/profiles.
- Writing abusive comments regarding current/previous Trust employees, governors, current/previous pupils or parents/guardians.
- Harassing or bullying current/previous Trust employees, or any persons unrelated or related to the Trust through cyber bullying and social exclusion.
- Viewing or updating personal social media account/profile (on Facebook, Twitter, Instagram, Snapchat etc) during the working day, unless on a designated break. (This includes via a work or personal mobile telephone and/or iPad).
- By proxy, updating their personal social media account/profile (Facebook, Twitter, Instagram, Snapchat etc) during their normal working day, and must ensure that their social media site/application is secure at all times from third parties.
- Accessing or sharing illegal material.
- Publishing any content, which may be deemed as defamation or discrimination
- Posting any images of pupils from the school or any other previous education establishment where the employee has worked.
- Without permission, posting any images of Trust employees on social media sites/applications from the Trust or any other previous education establishment where the employee has worked.
- Setting up and/or using an alias social media account to circumvent the policy.
- Commenting/posting/sharing any material which could bring the school into disrepute.
- Breaching any of the Trust's or school's other policies and procedures such as the Trust's Code of Conduct, Bullying and Harassment Policy, Equal Opportunities Policy.
- Using social media sites/applications as a forum for raising and escalating concerns regarding our school or the Trust. These concerns should be raised through the line manager or using the Grievance Procedure or the Whistleblowing Procedure.

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

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

5.1 Access to School ICT facilities and materials

Working with the Trust, the school's [network manager/ICT manager/school business manager (SBM)/etc.] manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

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

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the school's [network manager/ICT manager/school business manager (SBM)/etc.].

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

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy as it applies to staff.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff should enable multi-factor authentication on their email account(s).

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

Staff must not share their personal i.e. non-work issued email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. School email accounts should be used at all times

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 the email contains information that may give rise to a safeguarding concern, the member of staff must inform the school's designated safeguarding lead.

If staff send an email in error that contains the personal information of another person, they must inform the school's Data Protection Officer immediately and follow our data breach procedure.

Staff must not give their personal i.e. non-work issued phone number(s) to parents/carers or pupils. At all times staff must use phones and/or phone numbers provided by the school to conduct all work-related business. If staff have been provided with a VOIP telephone number which is mobile and accessed via an appropriate app, staff may use their own personal device to access this service.

School phones must not be used for personal i.e. non work related matters.

Staff personal devices must not be added to school supplied Wi-Fi

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.

If relevant add:

The school can record incoming and outgoing phone conversations.

If you record calls, callers **must** be made aware that the conversation is being recorded and the reasons for doing so. Your school's phone system probably has an automated option you can use/adapt.

Explain when you record phone conversations and why. For instance:

- "All calls to the school office are recorded to aid administrators"
- "Calls are recorded for use in staff training"

If relevant, add:

Staff who would like to record a phone conversation should speak to [insert relevant staff member and contact details].

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

Set out your protocol for approving requests here. For instance, you may grant requests to record conversations when:

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

5.1.2 Use of Social Media

There are two different forms of communication: personal communications and professional communications.

Personal communications are those made via a personal social media account. Personal communications that demonstrate a failure to follow professional standards or could damage the reputation of the school and Trust are within the scope of this policy.

Professional communications are those made through official channels, posted on a school social media account, or using the name of the school or Trust. All professional communications are within the scope of this policy.

If your school has official social media accounts, adapt this section, otherwise, delete it.

The school has an official [Facebook/Twitter/etc.] account, managed by [insert relevant member(s) of staff]. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The Trust and our school have 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 those guidelines at all times.

Personal Use of Social Media Sites and applications

Employees, volunteers and casual workers are reminded that they are entitled to undertake private conversation on social media sites and applications. However, employees must accept that if the conversation becomes public and the content is deemed to be inappropriate and/or unprofessional, disciplinary action may be undertaken.

For the purposes of this policy, social media is any online platform or any application that allows parties to communicate instantly with each other or to share data in a public forum. This includes social media forums such as X, Facebook, Instagram, Snapchat, LinkedIn and Reddit. Social media also covers blogs, and video / image-sharing websites such as YouTube. It further covers gaming platforms (such as Minecraft, World of Warcraft etc), online discussion groups, dating sites, and gambling sites. It also covers other forms of electronic communication software/applications such as texting, SMS, WhatsApp, and Facebook Messenger.

Employees should be aware that there are many more examples of social media than can be listed here and it is a constantly changing area, therefore, the examples listed are not an exhaustive list. Employees should follow the guidelines in Appendix 1 in relation to any social media and appropriate security settings that they use.

Employees, volunteers and casual workers should ask themselves the following question “if this conversation became public knowledge could it raise questions about my integrity or suitability to work in a school or Trust and could it bring the school or Trust into disrepute?”

5.2 Personal use of School ICT facilities and materials

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. This usage should be in line with the Trust Cyber Security Protocol document specifically in relation to BYOD (bring your own device).

Personal use is permitted provided that such use:

- Does not take place during non-break time
- Does not constitute ‘unacceptable use’, as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

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

Staff should be aware that use of the school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT monitoring activities (see section 5.4). Where breaches of this policy are found, disciplinary action may be taken

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

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

5.3 Remote access

If your school provides remote access facilities for staff, adapt this section. Otherwise, delete it and renumber the subsections below.

We allow staff to access the school's ICT facilities and materials remotely. If your school has one, add: They should dial in using a virtual private network (VPN).

Explain the remote access system you use, including:

- Who manages it
- Security arrangements
- Protocols for remote access
- How staff can request remote access

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and must take such precautions as the [network manager/ICT manager/SBM/headteacher/etc.] 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.

Add a link to your school's data protection policy here, or explain where it can be found.

5.4 Monitoring and filtering of the Trust and school network and use of ICT facilities

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

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

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

ICT use in our schools and Trust offices is monitored in order to:

- Obtain information related to school business
- Investigate compliance with school policies, procedures and standards
- Ensure effective school and ICT operation
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation

Our Trust 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
- Any approved AI tools for schools meet the DfE's product safety expectations.

The Trust'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 Trust's DSL and ICT Operations Manager, as appropriate.

5.5 Communicating with or about the school online

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

Parents/carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents/carers to sign the agreement in appendix 3.

5.6 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 pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

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

6. 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 in every school and in the Trust's Central Offices. 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 cybercrime 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

6.1 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 pupils who disclose account or password information may face disciplinary action. Parents, visitors or volunteers who disclose account or password information may have their access rights revoked.

6.2 Software updates, firewalls and anti-virus software

All of the Trust's and 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 Trust's and school's ICT facilities.

6.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

6.4 Access to facilities and materials

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

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 [insert relevant person] 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.

6.5 Encryption

The Trust makes sure that its devices and systems in use in each of its schools have an appropriate level of encryption.

School staff may only use personal devices (including computers and phones) to access school data, work remotely, or to take it out of the school premises if they have been specifically authorised to do so.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

7. Protection from cyber attacks

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

The Trust will:

- Work with schools, governors and our IT managed service provider to make sure cyber security is given the time and resources it needs to make the Trust and our schools secure

- Provide annual training for staff (and include this training in any induction for new starters) 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 IT systems need 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 Trust 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 Trust or a school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as effective and secure as they can be
- Backup critical data
- Complete external vulnerability testing and Phishing exercises
- Delegate specific responsibility for maintaining the security of our management information system (MIS)
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like Trust or 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 Trust's IT Managed Service provider including, for example, how the Trust 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 and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

8. Internet access

The internet connection provided by our Trust and to our school is secure.

8.1 Visitors

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

The headteacher will only grant authorisation if parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA).

Add any other circumstances where parents/carers or visitors will be granted access to the internet.

The school will only grant authorisation to other visitors if they need to access the school's WiFi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation).

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

9. Monitoring and Review

The headteacher and [ICT manager/network manager/SBM/etc.] monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every year.

The Board of Trustees is responsible for approving this policy.

10. Related Policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education
- Mobile phone usage
- Cyber Security Protocol
- AI Policy

Appendix 1: Personal use of all social media platforms, including management of privacy settings

Trust employees must be aware that everything posted online is public in nature, even with the strictest privacy settings. Once something is online, it can be copied and redistributed. Therefore, it should be assumed that everything that is written online is permanent and could be shared. All information posted online is subject to Copyright, General Data Protection Regulation legislation and the Safeguarding Vulnerable Groups Act 2006

All employees are reminded that they are bound by the Trust's Code of Conduct, and teaching staff are further subject to the Teachers' Standards. Under the Safeguarding Vulnerable Groups Act 2006 school employees may be referred to the Disclosure and Barring Service (DBS) where the Trust has significant concerns or suspicions about an employee's conduct or behaviour.

All employees are responsible for any content displayed/shared/posted on their social media accounts/applications, and as such must ensure that their privacy settings are updated and maintained appropriately and passwords are kept secure and confidential.

Trust employees, volunteers and casual workers should at all times:

- Have the highest standards of personal conduct (inside and outside of Trust)
- Ensure that their behaviour (inside and outside of Trust) does not compromise their position within the Trust
- Ensure that their judgement and integrity should not be able to be brought into question.
- Ensure that their relationship with members of the community, via social media, does not compromise their position within the Trust or bring into question their suitability to work with children and young people.

12 rules for Trust staff on the personal use of social media

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 without permission
5. If it is likely that you may be identified as a member of CLT staff don't share anything publicly that you wouldn't be happy showing our pupils and parents, or presenting in a classroom
6. Remember our professional standards of political impartiality, behaviour and staff code ofconduct.
7. Don't use social media during school hours unless for Trust marketing purposes
8. Don't make adverse comments about your job, your colleagues, our school, the Trust or our pupils online – once it's out there, it's out there
9. Don't associate yourself with the school or Trust on your profile unless you can comply with these rules for school staff on the personal use of social media
10. Don't link your work email address to your personal social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
11. Consider pausing any personal social media apps on your personal devices when in school if it recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)
12. Do not accept friend requests from students

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/carers. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the Trust's senior leadership team 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
- Pupils 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 pupil 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.
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.

TERM	DEFINITION
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.

Appendix 3: Acceptable use of the internet: agreement for parents and carers

Adapt this agreement to reflect the online communication channels your school uses, or to address any common issues with parent communication online.

Acceptable use of the internet: agreement for parents and carers
Name of parent/carer: **Name of child:**
Online channels are an important way for parents/carers to communicate with, or about, our school. The school uses the following channels: ● Our official Facebook page ● Email/text groups for parents (for school announcements and information) ● Our virtual learning platform Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- Be respectful towards members of staff, and the school, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure

I will not:

- Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way
- Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers

Signed:	**Date:**