ICT and internet acceptable use policy

Children of Success Trusts Trust

Key Changes/Update sfrom previous policy	
Identifcation of key users	This policy has sections specific to various groups of users namely staff, pupils and parents in line with recent upgrades to WiFi network in line with DfE/ ESFA guidlines
Section 5.5 - Monitoring of the Trust's network	As part of monitoring requirements in KCSIE and the general protection of the Trust's network
Section 9 – Protection Against Cyber security	Keeping policy in line with Risk mProtection Arrangemnet (RPA) insurance requirement
Action Required	FGPC to review and approve policy

Approved by:	FGPC	**Date:** July 2024
Next review due by:	July 2027	

Contents

1. Introduction and aims 3
2. Relevant legislation and guidance 3
3. Definitions 3
4. Unacceptable use 4
5. Staff (including trustees, governors, volunteers, and contractors) 5
6. Pupils 8
7. Parents 10
8. Data security 10
9. Protection from cyber attacks 12
10. Internet access 13
11. Monitoring and review 13
12. Related policies 13
Appendix 1: Facebook cheat sheet for staff 15
Appendix 2: Acceptable use of the internet: agreement for parents and carers 17
Appendix 3: Acceptable use agreement for older pupils 18
Appendix 4: Acceptable use agreement for younger pupils 19
Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors 20
Appendix 6: Glossary of cyber security terminology 21

Contents

1. Introduction and aims

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

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents and governors and trustees
- 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 our Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary 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, governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the 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 the Trust'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 risks bringing the Trust into disrepute
- Sharing confidential information about the Trust, 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
- 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 Executive Headteacher (EHT) or Finance Director and Operations Manager (FDOM) 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 the Trust 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 EHT's discretion.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's policies on [behaviour/discipline/staff code of conduct/etc.].

Copies of these policies can be found on the staff shared drive of each school.

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

5.1 Access to Trust ICT facilities and materials

The Trust's ICT partners, Executive Headteacher (EHT), Finance Director and Operations Manager (FDOM) and Heads of School (HoS) manage access to the Trust's ICT facilities and materials for Trust 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 Trust'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 FDOM and HoS as applicable.

Requests for access to files will be reviewed regularly and built into role profiles across the Trust however if access to certain files are required as part of a role, this request should be made by the HoS and approved by the FDOM.

5.1.1 Use of phones and email

The Trust 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 communication should be conducted using the email address the Trust has provided.
- Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

- If staff send an email in error that contains the personal information of another person, they must inform the FDOM immediately and follow our data breach procedure.
- Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the Trust 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 Trust ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Executive Headteacher or FDOM may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/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 Trust'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 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.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the Trust's conditions stated above.

Staff 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 and parents could see them.

Staff 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 should make sure their use of social media, either for work or personal purposes, is appropriate at all times.

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

5.3 Remote access

We allow staff to access the Trust's ICT facilities and materials remotely. They should dial in using the remote desktop connection (RDP) or securely through Bitlocker, managed by our ICT partners. Please speak to ICT Support or the FDOM if you have issues with remote access

Staff accessing the Trust'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 Trust's ICT facilities outside the Trust and take such precautions 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.

The Trust's data protection policy can be found in the staff shared areas.

5.4 Trust social media accounts

Though the Trust has no official social media pages, there are historic Facebook and Twitter accounts that are no longer in use and this section will be updated as and when these change.

5.5 Monitoring and filtering of the Trust 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

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

The Trust uses Sophos and Senso to filter and monitor online use and weekly reports on blocked searches are generated for review and investigation as applicable.

The effectiveness of any filtering and monitoring is regularly reviewed.

Where appropriate, authorised personnel may raise concerns about monitored activity with the Trust's designated safeguarding lead (DSL) and FDOM, as appropriate.

The Trust monitors ICT use in order to:

- Keep our pupils, staff and other Trust users safe
- Obtain information related to Trust business
- Investigate compliance with Trust policies, procedures and standards
- Ensure effective 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

The Finance and General Purposes Committee (FGPC), on behalf of the Trust Board will regularly review the effectiveness of the Trust's monitoring and filtering systems.

6. Pupils

6.1 Access to ICT facilities

The following are available for to pupils to access under supervision

- "Computers and equipment in classrooms and the Trust's ICT suite are available to pupils only under the supervision of staff"
- "Pupils will be provided with an account linked to the Trust's Student environment, which they can access from any Trust configured pupil device;

6.2 Search and deletion

Under the Education Act 2011, the headteacher, and any member of staff authorised to do so by the Executive headteacher, 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 Trust rules as a banned item for which a search can be carried out (your behaviour policy should list these items), **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 HoS or Designated safeguarding lead (DSL).
- 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, you should proceed according to your behaviour policy)

The authorised staff member should:

- 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. A list of banned items is available
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine 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 Trust 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 of School / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding 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
- Our behaviour policy / searches and confiscation policy (make sure that your searches and confiscation policy reflects the updated DfE guidance, which came into force on 1 September 2022)

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the Trust complaints procedure.

6.3 Unacceptable use of ICT and the internet outside of Trust

The Trust will sanction pupils, in line with the [behaviour/discipline policy], if a pupil engages in any of the following **at any time** (even if they are not on Trust 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'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 Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the 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 an employee, a volunteer/governor/ trustee or as a member of the PTA) may be granted an appropriate level of access, or be permitted to use the Trust's facilities in accordance with requirements of their role.

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

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 the Trust through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

7.3 Communicating with parents about pupil activity

The Trust 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 in the same way that information about homework tasks is shared.

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

Parents may seek any support and advice from the Trust 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-crime technologies.

Staff, pupils, parents and others who use the Trust's ICT facilities should use safe computing practices at all times. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the Trust'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.

Teachers will generate passwords for pupils using the required password manager or generator and keep these in a secure location in case pupils lose or forget their passwords.

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 must all be configured in this way.

8.3 Data protection

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

8.4 Access to facilities and materials

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

These access rights are managed by One Education, our ICT partners.

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 ICT and the FDOM immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

8.5 Encryption

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

School staff may only use personal devices (including computers and USB drives) to access Trust data, work remotely, or take personal data (such as pupil information) out of Trust if they have been specifically authorised to do so by the EHT and FDOM.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the Trust.

9. Protection from cyber attacks

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

The Trust will:

- Work with Trustees, governors and the IT partners to make sure cyber security is given the time and resources it needs to make the Trust secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Trust'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 Trust will verify this using a third-party audit (such as 360 degree safe) annually], 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 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 backup systems/external hard drives that aren't connected to the Trust network and which can be stored off the Trust premises.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to One Education, our outsourced ICT partners.
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like Trust email accounts
    - Store passwords securely using a password manager
- Make sure our ICT provider 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
- 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 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 either annually or after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The Trust's wireless internet connection is secure. For instance:

- The Trust uses Sophos and Senso filtering software to monitor and report attempted attacks with weekly reports generated
- The Trust has recently upgraded its Wi-Fi and internet infrastructure including separate connections for staff, pupils and guests

10.1 Pupils

- Pupils will access computer devices only under supervision and all pupil devices are on a pupil Wi-Fi network which is password protected

10.2 Parents and visitors

Parents and visitors to the Trust will not be permitted to use the Trust's Wi-Fi unless specific authorisation is granted by a member of the senior leadership team. This network is separate from the main Trust network and also password protected.

This will only grant authorisation if:

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

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 FDOM and ICT partners monitor 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 t**wo** years, unless there is a significant change in reporting needs, ICT risks or guidance from regulatory bodies.

The FGPC is responsible for reviewing/approving this policy.

12. Related policies

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

- Online safety
- Social media

- Safeguarding and child protection
- Behaviour
- Staff code of conduct
- Data protection
- Remote education
- Mobile phone usage

Appendix 1: Facebook cheat sheet for staff

Do not accept friend requests from pupils on social media

10 rules for Trust 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 Trust hours
7. Don't make comments about your job, your colleagues, our Trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the Trust on your profile (e.g. by setting it as your workplace, or by 'checking in' at a Trust 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 Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi 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 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 1 parent's friend request or message might set an unwelcome precedent for both you and other teachers at the Trust
    - 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 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 of the internet: agreement for parents and carers

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 Trust. The Trust uses the following channels: • Email/text groups for parents (for Trust 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 Trust via official communication channels, or using private/independent channels to talk about the Trust, I will: • Be respectful towards members of staff, and the Trust, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the Trust's official channels, so they can be dealt with in line with the Trust's complaints procedure I will not: • Use private groups, the Trust's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the Trust can't improve or address issues unless they are raised in an appropriate way • Use private groups, the Trust's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the Trust 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:**

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the Trust's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When using the Trust's ICT facilities and accessing the internet in Trust, I will not: • Use them for a non-educational purpose • Use them without a teacher being present, or without a teacher's permission • Use them to break Trust rules • Access any inappropriate websites • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity) • Use chat rooms • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video • Share my password with others or log in to the Trust's network using someone else's details • Bully other people I understand that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the Trust's ICT systems and internet responsibly. I understand that the Trust can discipline me if I do certain unacceptable things online, even if I'm not in Trust when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of Trust staff. I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and for using personal electronic devices in Trust, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the Trust's ICT facilities and internet: agreement for pupils and parents/carers	
Name of pupil:	
When I use the Trust's ICT facilities (like computers and equipment) and go on the internet in Trust, I will not: • Use them without asking a teacher first, or without a teacher in the room with me • Use them to break Trust rules • Go on any inappropriate websites • Go on Facebook or other social networking sites (unless my teacher said I could 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 • Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes • Share my password with others or log in using someone else's name or password • Bully other people I understand that the Trust will check the websites I visit and how I use the Trust's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules. I will tell a teacher or a member of staff I know immediately if I find anything on a Trust computer or online that upsets me, or that I know is mean or wrong. I will always be responsible when I use the Trust's ICT systems and internet. I understand that the Trust can discipline me if I do certain unacceptable things online, even if I'm not in Trust when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of Trust staff. I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and for using personal electronic devices in Trust, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 5: 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, volunteers and visitors	
Name of staff member/ trustee//governor/volunteer/visitor:	
When using the Trust's ICT facilities and accessing the internet in Trust, or outside Trust 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 Trust'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 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, its pupils 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 Trust	
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 Trust, and keep all data securely stored in accordance with this policy and the Trust's data protection policy. I will let the HoS and DSL 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 (staff member/governor/volunteer/visitor):	**Date:**

Appendix 6: 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're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.

TERM	DEFINITION
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.