ICT and internet acceptable use policy

Heritage MAT

Approved by:	[Heritage MAT Trust Board]	**Date:**	[23.02.26]
Last reviewed on:	[23.02.26]		
Next review due by:	[February 2027]		

Contents

1. Introduction and aims 2
2. Relevant legislation and guidance 3
3. Definitions 3
4. Unacceptable use 3
5. Staff (including governors, volunteers, and contractors) 5
6. Pupils 8
7. Parents/carers 9
8. Data security 9
9. Protection from cyber attacks 10
10. Internet access 12
11. Monitoring and review 12
12. Related policies 12
Appendix 1: Acceptable use of the internet: agreement for parents and carers 13
Appendix 2: Acceptable use agreement for older pupils 14
Appendix 3: Acceptable use agreement for younger pupils 15
Appendix 4: Acceptable use agreement for staff, governors, volunteers and visitors 16
Appendix 5: Glossary of cyber security terminology 17

+

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 (including the senior leadership team), governors, 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.

This policy aims to:

- Set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents/carers and governors
- 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, visitors, and anyone who has access to our IT and communication systems.

Misuse of IT and communications systems can damage our Trust and our reputation. Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct/AI policy.

2. Relevant legislation and guidance

This policy refers to, complies with, or otherwise has regard to, 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
- Data (Use and Access) Act 2025
- 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 2025
- Searching, screening and confiscation: advice for Trusts 2022
- National Cyber Security Centre (NCSC): Cyber Security for Trusts
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in Trusts and colleges

3. Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the Trust's ICT service
- **Users:** anyone authorised by the Trust to use the Trust's ICT facilities, including 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 5 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 any web page or downloading any image, document, application, or file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste, or immoral
- 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
- Using the Trust's systems to participate in internet chat rooms, post on internet message boards or blogs, unless approved by authorised personnel
- 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 internet and 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
- Inappropriate use of AI (See policy)

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The relevant headteacher 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 headteacher's discretion. Approval should be sought from the relevant headteacher.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust's policies on behaviour/staff discipline/staff code of conduct. Copies of relevant policies can be found on the individual school's website.

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

5.1 Access to Trust ICT facilities and materials

The Individual school's network manager/ICT manager manages access to the Trust's ICT facilities at school level 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 relevant lead.

5.1.1 Use of Trust-supplied equipment

Trust-issued devices (including laptops, tablets and other digital devices) are provided to staff for the purpose of supporting teaching, learning and the efficient running of the Trust. All Trust-supplied equipment remains the property of the Trust and staff must return the equipment at the end of employment, or when it is no longer required. Staff must:

- Use equipment and devices primarily for Trust purposes and in line with the Trust's policies on safeguarding, data protection and confidentiality
- Store devices securely when not in use, particularly when travelling. Devices should not be left unattended in public places or in unsecured locations
- Be actively aware of data security and confidentiality and follow best practice when accessing the equipment away from Trust. E.g. when travelling on public transport, be aware that other passengers may be able to read any documents displayed on the screen of your device
- Lock devices with a password when unattended. Passwords must:
  - Not be shared with others and must be changed regularly
  - Be suitably strong, in accordance with the Trust's password policy (see section 8.1)
  - Not be reused across multiple accounts
- Update software, operating systems and applications when prompted, or as directed by the relevant lead
- Connect to the Trust network using approved and secure methods. When connecting to wi-fi networks outside of the Trust, staff must ensure connections are secure and avoid transmitting sensitive data over public or unsecured networks
- Report any loss, theft, damage or compromise of a Trust device promptly to the relevant IT lead, designated safeguarding lead and data protection officer

5.1.2 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 must make sure multi-factor authentication is enabled on their email account(s).

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

Staff must not share their personal email addresses with parents/carers 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 subject access requests from individuals under the UK GDPR and 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 using a strong, state-of-the-art encryption standard 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 relevant lead immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents/carers or pupils. In circumstances where staff are provided with phones, these staff must use the phones provided by the Trust to conduct all work-related business.

Trust 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.

Some schools in the Trust can record incoming phone conversations. Phone users are made aware of this feature for incoming calls.

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

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 relevant lead 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
- 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 policies.

Staff may not store any Trust-related data on personal devices, on cloud storage or on personal removable storage devices.

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/carers could see them.

Staff should take care to follow the Trust's guidelines on use of social media and use of email (see section 5.1.2) 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.

5.3 Remote access

We allow staff to access the Trust's ICT facilities and materials remotely where individual schools allow this. They should dial in using the relevant access portal.

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 must take such precautions as the relevant lead may require against importing viruses or compromising system security.

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

5.4 Trust social media accounts

Each school in our Trust has official social media accounts. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

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

To comply with Department for Education (DfE) guidance on meeting digital and technology standards, and 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 reserves the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Trust, including for the following purposes

- To monitor whether the use of the email system or the internet is legitimate and in accordance with this policy
- To find lost messages or retrieve messages lost due to computer failure
- To help in the investigation of alleged wrongdoing
- To comply with any legal obligation

The list above is not exhaustive.

The Trust monitors ICT use in order to:

- 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

Our Trust Board is responsible for making sure that:

- The Trust meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
  - For the leadership team and relevant staff, this includes how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the Trust's monitoring and filtering systems

The individual school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the Trust's DSL and ICT manager, as appropriate.

6. Pupils

6.1 Unacceptable use of ICT and the internet outside of Trust

The Trust will sanction pupils, in line with our the individual school's behaviour 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
- Inappropriate use of AI

7. Parents/carers

7.1 Access to ICT facilities and materials

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

However, parents/carers working for, or with, the Trust 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 Trust's facilities at the headteacher's discretion.

Where parents/carers are granted access in this way, they must abide by this policy.

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/carers 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/carers to sign the agreement in appendix 1.

7.3 Communicating with parents/carers 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/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 Trust pupils will be interacting with online, including the purpose of the interaction.

Parents/carers 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/carers 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 Trusts 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 must not use the same passwords across multiple platforms.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control. You must keep these passwords confidential and change them regularly.

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.

All staff will use the password manager required by the relevant school lead to help them store their passwords securely. 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 should not delete, destroy or modify existing systems, programs, information or data. Users must not download or install software from external sources without authorisation from the relevant school lead.

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 incoming files will always be virus-checked before they are downloaded.

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 the relevant school lead.

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 relevant school lead 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.

Trust 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 the Trust if they have been specifically authorised to do so by the headteacher.

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

9. Protection from cyber attacks

Please see the glossary (appendix 5) to help you understand cyber security terminology.

The Trust will:

- Work with local governors and the IT department to make sure cyber security is given the time and resources it needs to make the Trust secure
- Provide ongoing training for all users, including staff, pupils and governors (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:
  - The methods hackers use for tricking people into disclosing personal information, including phishing
  - Online safety and password security

- Social engineering, including not using websites that host unsuitable material, and could also contain malware and viruses
- The physical security of devices, for example not leaving a laptop unlocked and unattended
- The risks of using removable storage media, such as USBs
- Multi-factor authentication
- How and when to report a cyber incident or attack
- How and when to report a data breach
- Data protection for all staff. Staff who are exposed to higher-risk data will have more frequent training
- How to check the sender address in an email
- How to respond to a request for bank details, personal information or login details
- How to 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 (data privacy impact assessment) 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

› Delegate specific responsibility for maintaining the security of our management information system (MIS) to each school's relevant lead

› Make sure staff:

- Dial into our network using approved methods
- Enable multi-factor authentication where they can, on things like Trust email accounts
- Store passwords securely

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

› Make sure all necessary firewalls are in place and switched on (and that all areas of the network are secured effectively)

› Make sure effective cyber breach prevention measures and processes are in place, e.g. endpoint detection and response systems

› 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 (or a similarly effective and recognised) certification

› Develop, review and test an incident response plan

› Conduct a cyber risk assessments

› Appoint a digital lead to oversee cyber risk assessment

10. Internet access

Each school's wireless internet connection is secure and managed by a filtering and monitoring ayatem. Inappropriate content will be blocked and reported to the relevant senior leader.

10.1 Parents/carers and visitors

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

The headteacher will only grant authorisation if:

- Parents/carers 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 WiFi 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 WiFi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Headteacher / Principal and relevant school lead will 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 annually.

The Trust Board is responsible for reviewing/approving this policy.

12. Related policies

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

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection
- Remote education
- Mobile phone usage
- Artificial Intelligence (AI)

Appendix 1: 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: • Social media • 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 Trust-related 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 2: 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 • Present AI-generated text or imagery as my own work • Use AI inappropriately 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 3: 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 • Present AI-generated text or imagery as my own work • Use AI inappropriately 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 4: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the Trust's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/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 any illegal or 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 any private business, 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 designated safeguarding lead (DSL) and ICT 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 (staff member/governor/volunteer/visitor):	**Date:**

Appendix 5: 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. Many of these terms are from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove viruses and other kinds of malicious software.
Breach	When your data, computer systems or networks are accessed or affected without authorisation.
Cloud	An on-demand, massively scalable service, hosted on a shared infrastructure 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	Any event that threatens the confidentiality, integrity, or availability of data within your computer network, or where the security of your system or service has otherwise been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from unauthorised 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 who uses their technology skills to gain unauthorised access to computers, systems and networks.
Malware	Malicious software. Any kind of software that can damage computer systems, networks or devices, which includes viruses, trojans or any code or content that is harmful.
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 with the end aim of fixing them.

TERM	DEFINITION
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 or text messages sent to many people asking for sensitive information (such as bank details or passwords) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems, usually by encrypting your files, until you make a payment (a ransom) for decryption.
Social engineering	Manipulating people into giving information or carrying out specific actions that's of use to an attacker.
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.