Acceptable Use Policy (ICT and e-Communications)

Date Published	**April 2024**
Version	**1**
Approved Date	**April 2024**
Review Cycle	**Annual**
Review Date	**February 2025**

"Learning together, to be the best we can be"

1. Aims

1.1. Information and communications technology (ICT) is an integral part of the way our Trust works, and is a critical resource for pupils, staff, governors, volunteers and visitors. However, the ICT resources and facilities our Trust uses could also pose risks to data protection, online safety and safeguarding.

1.2. This policy aims to:

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

1.3. This policy covers all users of our Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

1.4. Breaches of this policy may be dealt with under the Code of Conduct.

1.5. This policy replaces the Trust electronic communications policy, which was de-commissioned in April 2024.

2. Legislation

2.1. 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 2023
- Searching, screening and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in schools and colleges

3. Definitions

3.1. This policy uses the following definitions:

3.1.1. 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;

3.1.2. Users: anyone authorised to use the Trust's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors;

3.1.3. Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user;

3.1.4. Authorised personnel: employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities;

3.1.5. 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.

4. Unacceptable Use

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

4.2. Unacceptable use of the ICT facilities includes:

- 4.2.1. Using the ICT facilities to breach intellectual property rights or copyright;
- 4.2.2. Bully or harass someone else, or to promote unlawful discrimination;
- 4.2.3. Using the ICT facilities to breach the other policies or procedures;
- 4.2.4. Any illegal conduct, or activity which is deemed to be advocating illegal conduct;
- 4.2.5. Online gambling, inappropriate advertising, phishing and/or financial scams;
- 4.2.6. Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful;
- 4.2.7. Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams;
- 4.2.8. Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute;
- 4.2.9. Sharing confidential information about the Trust, its pupils, or other members of school communities;
- 4.2.10. Connecting any device to the ICT network without approval from authorised personnel;
- 4.2.11. Setting up any software, applications or web services on the 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 ICT facilities, accounts or data;
- 4.2.12. Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel;
- 4.2.13. Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the ICT facilities;
- 4.2.14. Causing intentional damage to the ICT facilities;

4.2.15. Removing, deleting or disposing of the ICT equipment, systems, programmes or information without permission from authorised personnel;
4.2.16. 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;
4.2.17. Using inappropriate or offensive language;
4.2.18. Promoting a private or personal business, unless permissions has been granted to do so;
4.2.19. Using websites or mechanisms to bypass the filtering or monitoring mechanisms
4.2.20. Engaging in content or conduct that is extremist, racist, or discriminatory in any other way;
4.2.21. Using AI tools and generative chatbots without permission;
4.2.22. During assessments, including internal and external assessments, and coursework (unless specifically allowed);
4.2.23. Any context where AI-generated content is presented as a pupil's own work.

4.3. This is not an exhaustive list. The Trust will use the professional judgement of its officers to determine whether any act or behaviour not on the list above is considered unacceptable use of the ICT facilities.

5. Staff (including governors, volunteers and contractors

5.1. The Trust ICT team manages access to the ICT facilities and materials for staff. That includes, but is not limited to:

5.1.1. Computers, tablets, mobile phones and other devices
5.1.2. Access permissions for certain programmes or files

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

5.3. 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 ICT Team.

5.4. The Trust provides each member of staff with a platform for electronic communications and an individual account, including email and other applications. This account should be used for work purposes only. Multi-factor authentication will be enabled on the account(s).

5.5. All work-related business should be conducted using the account and associated email address and identifiers that the Trust has provided.

5.6. Staff must not share their personal email addresses or contacts with parents/carers and pupils, and must not send any work-related materials using their personal accounts.

5.7. Staff must take care with the content of all communications, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

5.8. Communications 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/account does not mean that an email cannot be recovered for the purposes of disclosure. All communications should be treated as potentially retrievable.

5.9. Staff must take extra care when sending sensitive or confidential information. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

5.10. If staff receive a communication in error, the sender should be informed and the communication deleted. If the communication contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send a communication in error that contains the personal information of another person, they must immediately follow the Trust Data Protection Policy.

5.11. Staff must not give their personal phone number(s) to parents/carers or pupils, unless this has been pre-approved by their line manager. Staff must otherwise use phones provided by the school to conduct all work-related business. Trust\School Mobile phones must not be used for personal matters.

5.12. 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 this policy. The Trust can record incoming and outgoing phone conversations. This may be done to protect staff from abusive behaviour. This function may be used for safeguarding. All non-standard recordings of phone conversations must be pre-approved and consent obtained from all parties involved.

5.13. Staff are permitted to occasionally use Trust ICT facilities for personal use, subject to conditions set out in this policy. This permission must not be overused or abused, and must not be for any other business pursuit, including Trade Union activity. This may be withdrawn or permissions restricted at any time at the discretion of Headteachers or the central Executive Management Team.

5.14. Personal use is permitted provided that such use:

5.14.1. Does not take place during contact time/teaching hours/non-break time;
5.14.2. Does not constitute 'unacceptable use', as defined in this policy;
5.14.3. Takes place when no pupils are present;
5.14.4. Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

5.15. Staff must not use Trust ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos). Staff should be aware that use of the ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

5.16. 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.

5.17. Staff should take care to follow the Trust's guidelines on use of social media (appendix 6) and other digital communications to protect themselves online and avoid compromising their professional integrity.

6. Personal social media accounts & digital communication

6.1. Members of staff should make sure their use of social media, either for work or personal purposes, is appropriate at all times and would not risk compromising their own professional integrity or bringing the Trust into disrepute, and be consistent with the Nolan Principles/

6.2. The Trust allows access to the wireless network by personal devices if the device complies with security standards set out by the Trust. Devices must run supported operating systems on manufacturer-supported hardware and should have antivirus and firewalls in place. The devices must not have inappropriate software running and should not attempt to bypass the filtering systems used by the Trust. Devices are the responsibility of the owner, and any damage incurred on-site is their responsibility. Trust data should not be moved and stored on personal devices.

6.3. Staff are permitted to access files and email using their personal devices as long as they are secured with a pin code\password. The Trust reserves the right to remove or block devices from the network if appropriate. The Trust operates monitoring and filtering systems that may record information from devices accessing the Trust wireless network.

6.4. We allow staff to access the Trust ICT facilities and materials remotely. Staff can access cloud-based systems through their usual account access or, where necessary, should dial in using the Trust's virtual private network (VPN).

6.5. Access to Trust systems and the VPN is managed by the ICT team. Staff can request access via the IT helpdesk.

6.6. Staff accessing the Trust ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Staff must be particularly vigilant if they use the Trust ICT facilities outside the Trust\school.

7. School social media accounts

7.1. If schools utilise official social media accounts, managed by staff, these should be limited to a minimal reasonable number. Staff members who have not been authorised to manage or post to the account must not access or attempt to access the account. Accounts must be set up using the Trust email address or equivalent and should never be managed through personal accounts. The Data Controller and Processor must keep a record of who is managing accounts within

their schools and ensure that appropriate systems are in place to enable management of those accounts in the event of staff absence.

7.2. Staff managing social media accounts connected to the Trust/school must ensure that every post is in line with this policy, is purposeful, appropriate, and is in line with the Trust/school vision and values and consistent with the code of conduct. Staff managing accounts are advised to remove old posts at the end of each academic year, therefore no publicly-accessible posts/images should ever be more than 12 months old. Those who are authorised to manage, or post to, the account must make sure they abide by these requirements at all times.

8. Monitoring and filtering of the network and use of ICT facilities

8.1. 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

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

8.3. The Trust monitors ICT use 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

8.4. The Chief Executive Officer is responsible for making sure that:

8.4.1. The Trust meets the government's filtering and monitoring standards;
8.4.2. Appropriate filtering and monitoring systems are in place;
8.4.3. Staff are aware of those systems and trained in their related roles and responsibilities. For school leadership teams and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns;
8.4.4. The effectiveness of the Trust's monitoring and filtering systems is reviewed regularly.

8.5. Each school's designated safeguarding lead (DSL) will take lead responsibility for understanding the filtering and monitoring systems and processes that are in place.

8.6. Where appropriate, staff may raise concerns about monitored activity with the school's DSL, their line manager or ICT team, as appropriate.

9. Pupils use of ICT

9.1. Computers and ICT equipment in school are available to pupils only under the supervision of staff.

9.2. Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the 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 school rules as a banned item for which a search can be carried, and/or
- Is evidence in relation to an offence

9.3. 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)

9.4. 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 Headteacher or 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

9.5. 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.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk.

9.6. Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a justifiable reason to do so only with the express permission of the information controller (Headteacher).

9.7. When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

9.8. If inappropriate material is found on the device, the staff member must engage with the DSL and the headteacher should 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.

9.9. When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. The erasing of data or files from a device that is not Trust-owned must be approved by the Headteacher, and the Trust Data Protection Officer informed. Advice from the DSL should also be sought if this relates to matters of a safeguarding nature. If the material is not suspected to be evidence in relation to an offence, the Headteacher may determine to delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- It is the only way to protect the integrity and legal right to anonymity of the pupils or staff in a school, without otherwise referring the matter to the Police and the Information Commissioners Office;
- The pupil and/or the parent refuses to delete the material themselves

9.10. In circumstances where the pupil and/or parent refuses to enable access to a device for the purposes of review or deletion, and the Headteacher is clear that there is a requirement to examine data or files on a device to ensure the Trust meets its legal Data Protection duties, the device will be retained on the school site until the issue is resolved, and parents/carers will be signposted to the Trust Complaints Policy where they disagree.

9.11. 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 Government's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The latest statutory guidance on searching, screening and confiscation

- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

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

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

9.14.1. Using school/Trust ICT to breach intellectual property rights or copyright

9.14.2. Using school/Trust ICT to bully or harass someone else, or to promote unlawful discrimination

9.14.3. Breaching the school's policies or procedures

9.14.4. Using school/Trust ICT for any illegal conduct, or making statements which are deemed to be advocating illegal activity

9.14.5. Using school/Trust ICT to access, create, store, link to or communicate material that is pornographic, offensive, obscene or otherwise inappropriate

9.14.6. Using school/Trust ICT for 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)

9.14.7. Activity which defames or disparages the school/Trust, or risks bringing the school/Trust into disrepute

9.14.8. Sharing confidential information about the school, other pupils, or other members of the school community

9.14.9. Gaining or attempting to gain access to restricted areas of the Trust/school network, or to any password-protected information, without approval from authorised personnel

9.14.10. Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities

9.14.11. Causing intentional damage to the Trust/school's ICT facilities or materials

9.14.12. 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

10. Parents/Carers

10.1. Parents/carers do not have access to the Trust/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.

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

10.3. 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/digital channels.

10.4. We therefore ask parents/carers to sign the agreement in appendix 2.

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

10.6. 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.

10.7. 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.

11. Data Security

11.1. 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 cybercrime technologies.

11.2. 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 Government'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

11.3. 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.

11.4. 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.

11.5. 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.

11.6. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards the Trust implement and maintain to protect personal data and the Trust's ICT facilities.

11.7. Any personal devices using the Trust's network must all be configured in this way.

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

11.9. All users of the Trust's ICT facilities will have clearly defined access rights to school systems, files and devices. These access rights are managed by the ICT Team in conjunction with line managers.

11.10. 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 ICT Team and their line manager immediately.

11.11. 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.

11.12. The Trust makes sure that its devices and systems have an appropriate level of encryption. Staff may only use personal devices (including phones, computers and USB drives) to access Trust data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher or equivalent.

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

12. Protection from cyber attacks

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

12.2. The Trust will:

12.2.1. make sure cyber security is given the time and resources it needs to make the Trust secure

12.2.2. Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:

12.2.2.1. Check the sender address in an email
12.2.2.2. Respond to a request for bank details, personal information or login details
12.2.2.3. Verify requests for payments or changes to information

12.2.3. Make sure staff are aware of its procedures for reporting and responding to cyber security incidents

12.2.4. Investigate whether our IT software needs updating or replacing to be more secure

12.2.5. Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data

12.2.6. Put controls in place that are:

12.2.6.1. Proportionate: the school will verify this periodically through external audit to objectively test that what it has in place is effective

12.2.6.2. Multi-layered: everyone will be clear on what to look out for to keep our systems safe

12.2.6.3. Up to date: with a system in place to monitor when the school needs to update its software

12.2.6.4. Regularly reviewed and tested: to make sure the systems are as effective and secure as they can be

12.2.7. Back up critical daily and store these backups in cloud based storage.

12.2.8. Delegate specific responsibility for maintaining the security of our management information system (MIS) to our Cloud based provider.

12.2.9. Make sure staff:

12.2.9.1. Dial into our network using a virtual private network (VPN) when working from home

12.2.9.2. Enable multi-factor authentication where they can, on things like school email accounts

12.2.9.3. Store passwords securely

12.2.10. 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

12.2.11. Have a firewall in place that is switched on

12.2.12. 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

12.2.13. Develop, review and test an incident response plan with the IT department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and

when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

13. Internet Access

13.1. The school's wireless internet connection is secure. All SSID's are filtered to either staff or pupil appropriate levels. Guest wireless is available at some sites, this is filtered and monitored.

13.2. If staff become aware of sites that they believe should have been filtered out of Trust systems, they should inform their line manager and the ICT team immediately and, where appropriate, the DSL.

13.3. Pupils can access the wireless using school devices.

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

13.5. 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)
- Visitors 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 or lesson plan)

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

APPENDIX 1

Acceptable use of ICT: 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 a variety of channels for digital communication with parents/carers. 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:**

APPENDIX 2

Acceptable use of the school's ICT facilities and internet: agreement for older pupils and their parents/carers

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, 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 school 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 inappropriate 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 school's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots:
    - During assessments, including internal and external assessments, and coursework (unless specifically allowed)
    - Any context where AI-generated content is presented as a pupil's own work

I understand that the school will monitor the websites I visit and my use of the school'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 school's ICT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 3

Acceptable use of the school's ICT facilities and internet: agreement for younger pupils and their parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers, tablets and equipment) and go on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless 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
- Use artificial intelligence (AI) to create images or write for me, and then submit it as my own work

I understand that the school will check the websites I visit and how I use the school's computers, tablets 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 computer or online that upsets me, or that I know is mean or wrong.

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

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

APPENDIX 4

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

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

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

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. Misuse or loss of communications equipment due to negligence will result in employees being requested to reimburse costs to the Trust and may result in disciplinary action.

I will let the designated safeguarding lead (DSL) and ICT team 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 school's ICT systems and internet responsibly, in line with the Trust's policies, and ensure that pupils in my care do so too. I understand that anything I access or send is of a legitimate business need, does not breach copyright or data protection, complies with other Trust policies and is respectful, courteous and professional. I will use my mobile phone for multifactor authentication and not personal use during lesson time.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

APPENDIX 5: Cyber Security Glossary

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.

TERM	DEFINITION
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.
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.

TERM	DEFINITION
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 6: Social Media Guidelines

The Trust recognises that social media and social networking sites play an important role in the lives of many people, including our employees, pupils and parents.

The Employee Code of Conduct gives clarity to the way in which social media is to be used by staff employed by the Trust, and whilst social media gives many benefits, there are also associated risks around safeguarding and reputational damage in an educational environment.

It is likely that a high proportion of our staff have their own social networking site accounts. It is important for them to protect their professional reputation by ensuring that they use their personal accounts in an appropriate manner.

We therefore ask that all staff review and adjust their privacy settings to give them the appropriate level of privacy and confidentiality. Please ensure that any social media accounts are set to 'private' and due consideration is given to anything posted on a social media account which may be deemed inappropriate.

Inappropriate posts could include those which contain extreme views, hate and discriminatory behaviour, illegal activities, sexually explicit/violent content or inappropriate/undesirable content such as swearing.

Further guidelines on the use of personal social media accounts are issued as follows:

- Staff must never add pupils as 'friends' into their personal accounts (including past pupils under the age of 16). Staff should only use school-authorised accounts or platforms when corresponding with pupils, parents, carers
- Staff are strongly advised not to add parents/carers as 'friends' into their personal accounts
- Staff must not post photographs or comments about the Trust, school(s), pupils, parents/carers or colleagues including members of the Trust Board and/or local governance
- Staff must not use social networking sites (for personal use) within work hours
- Inappropriate use by staff of social media should be referred to the Headteacher as soon as possible. This may lead to disciplinary action being taken.

In line with Keeping Children Safe in Education guidance, our recruitment activities

across the Trust and schools now factor in an 'online social media check' for all new applicants to identify any issues which may need exploring prior to offering employment.

If you have any queries on the above guidance, please contact the Central Trust HR Team on 01709 257277 or by email to hr-enquiries@nexusmat.org