

Inspiring Primaries Academy Trust

ICT and internet acceptable use policy for staff, parents & carers

**This policy applies to all the academies in Inspiring Primaries Academy
Trust**

Approved by:	Trust Board	Date: 6 March 2024
---------------------	-------------	---------------------------

Last reviewed on:	6 March 2024
--------------------------	--------------

Next review due by:	6 March 2027
----------------------------	--------------

Contents

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

1. Introduction and aims

Information and communications technology (ICT) is an integral part of the way our Trust and academies work, and is a critical resource for pupils, staff (including the senior leadership team), trustees, 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, parents/carers, trustees 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 trustees, governors, staff, 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 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

- **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 trustees, governors, staff, 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 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 head of school or any other relevant member of staff 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.

4.2 Sanctions

Staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the Trust's policies on staff disciplinary and staff code of conduct. Copies of these policies can be found on the IPAT Policies and Guidance Google drive.

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

5.1 Access to Trust ICT facilities and materials

The Trust's IT managed service provider (ekte) (supported by the central team) manages 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 ekte helpdesk (support@ekte.uk).

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 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 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; egress secure email is required to be used to send sensitive and confidential email.

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 school's data protection champion immediately and follow our data breach procedure by logging an incident on GDPRiS.

Staff must not give their personal phone number(s) to parents/carers or pupils. Staff must use 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.

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 headteacher/head of school 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 mobile phone policy.

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 (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.

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 IT service provider 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.

The Trust's data protection policy can be found in the IPAT Policies and Guidance Google drive.

5.4 Trust social media accounts

The Trust and its academies have official Facebook and Twitter accounts, managed by the executive principals and heads of school. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The Trust has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

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 personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law. The Trust uses Netsweeper (St. Margaret's CE Primary School, Stoke Golding) and iBoss filtering software (all other academies).

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

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

6. Parents/carers

6.1 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 as it applies to staff.

6.2 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 2.

6.3 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.

7. 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 schools and colleges](#), including the use of:

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

7.1 Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure. The Trust's password policy is available on the IPAT Policies and Guidance Google drive.

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

Members of staff 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 should use a password manager as recommended in the password policy to help them store their passwords securely.

7.2 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.

7.3 Data protection

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

7.4 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 ekte

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 data protection champion 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.

7.5 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 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.

8. Protection from cyber attacks

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

The Trust will:

- Work with trustees and the IT provider 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](#)) at least 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 automatically 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 our cloud-based provider
- Make sure staff:
 - Enable multi-factor authentication where they can, on things like Trust email accounts
 - Store passwords securely using a password manager
- Make sure system administrators 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 service provider including, for example, how the Trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify [Action Fraud](#) of the incident, if necessary. This plan will be reviewed and tested at least annually and after a significant event has occurred, using the NCSC's '[Exercise in a Box](#)'

9. Internet access

The Trust's wireless internet connection is secure. Filtering software is used for all internet access.

Staff should report inappropriate sites that the filter hasn't identified (or appropriate sites that have been filtered in error) to the DSL (or deputy) and ekte.

9.1 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/head of school.

The headteacher/head of school 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.

10. Monitoring and review

The Director of Finance and Operations and members of the senior leadership team 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 3 years.

The Trust board is responsible for reviewing and approving this policy.

11. Related policies

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

- E-safety
- Social media
- Safeguarding and child protection
- Staff disciplinary
- Data protection
- Remote education
- Mobile phones

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 profile picture to something unidentifiable, or if you don't, make sure that the image is professional
2. Check your privacy settings regularly
3. Be careful about tagging other staff members in images or posts
4. Don't share anything publicly that you wouldn't be happy showing your pupils
5. Don't use social media sites during school hours
6. Don't make comments about your job, your colleagues, our Trust or your pupils online – once it's out there, it's out there
7. 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)
8. 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
9. Consider uninstalling the Facebook app from your phone. The app recognises WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What to do if ...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents/carers. 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/carer adds you on social media

- It is at your discretion whether to respond. Bear in mind that:
 - Responding to 1 parent/carer's friend request or message might set an unwelcome precedent for both you and other teachers at the Trust
 - Pupils may then have indirect access through their parent/carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent/carer know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: 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:

- Our official X (Twitter) and Facebook pages
- Arbor email groups for parents (for Trust announcements and information)
- Our virtual learning platform, Google

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 staff, trustees, 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/trustee/governor/volunteer/visitor:

When using the Trust'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 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 school, and keep all data securely stored in accordance with this policy and the Trust's data protection policy.

I will let the designated safeguarding lead (DSL) and 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 4: 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-authorized way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank

TERM	DEFINITION
	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.