EQUITAS ACADEMIES TRUST

ICT & INTERNET ACCEPTABLE USE POLICY

Review Date:	**March 2023**
To be Reviewed:	**March 2026**
Agreed:	**F & GP**
Policy Lead:	**Strategic ICT & Network Manager**

ICT & Internet Acceptable Use Policy

Contents **Page(s)**

1. **Introduction & Aims** 3
2. **Relevant legislation and guidance** 3
3. **Definitions** 4
4. **Unacceptable Use** 4
   - 4.1 Exceptions from unacceptable use 5
   - 4.2 Sanctions 5
5. **Staff (including governors, volunteers and contractors)** 5
   - 5.1 Access to trust ICT facilities and materials 5
   - 5.2 Use of phones and emails 5
   - 5.3 Personal use 6
   - 5.4 Personal social media accounts 6
   - 5.5 Remote access 6
   - 5.6 Monitoring and filtering of the trust network and use of ICT facilities 7
6. **Pupils** 7
   - 6.1 Access to ICT facilities 7
   - 6.2 Search and deletion 7
   - 6.3 Unacceptable use of ICT and internet outside of trust 9
7. **Parents** 9
   - 7.1 Access to ICT facilities and materials 9
8. **Data security** 9
   - 8.1 Passwords 10
   - 8.2 Software updates, firewalls and anti-virus software 10
   - 8.3 Data protection 10
   - 8.4 Access to facilities and materials 10
   - 8.5 Encryption 10
9. **Protection from Cyber attacks** 10
10. **Internet Access** 11
    - 10.1 Parents and visitors 11
11. **Monitoring and Review** 12
12. **Appendix 3 – Acceptable use agreement for older pupils** 13
13. **Appendix 4 – Acceptable use agreement for younger pupils** 14
14. **Appendix 5 – Acceptable use agreement for staff, governors, volunteers and visitors** 15

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 and governors
- Establish clear expectations for the way all members of the 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 trusts in teaching pupils safe and effective internet and ICT use

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

Breaches of this policy may be dealt with under our staff behaviour policy.

2. RELEVANT LEGISLATION AND GUIDANCE

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- Searching, screening and confiscation: advice for trusts 2022
- National Cyber Security Centre (NCSC): Cyber Security for Trusts
- Education and Training (Welfare of Children) Act 2021
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Meeting digital and technology standards in 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 which may become available in the future which is provided as part of the trust's ICT service
- **Users:** anyone authorised by the trust to use the trust's ICT facilities, including 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

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.

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 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. Staff and students would gain approval for such activities by emailing the headteacher requesting permission and explain the reason for the request

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the trust's policies on behaviour. In addition access to the trust ICT facilities may be revoked.

5. STAFF (INCLUDING GOVERNORS, VOLUNTEERS, AND CONTRACTORS)

5.1 Access to trust ICT facilities and materials

The trust's Strategic ICT Network & Systems Manager 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 It Support team by sending an email to the support email address.

5.2 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 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 and pupils, and must not send any work-related materials using their personal email account.

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

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

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

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the headteacher and the Strategic ICT Network & Systems Manager immediately and follow our data breach procedure.

Staff must not give their personal phone number(s) to parents or pupils. Staff must use phones provided by the trust to conduct all work-related business.

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.

5.3 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 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 teaching hours
- 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. Where breaches of this policy are found, disciplinary action may be taken.

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

5.4 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.

5.5 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 take such precautions as the Strategic ICT Network & Systems Manager 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 has an official Facebook and Instagram account, 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.

5.6 Monitoring and filtering of the trust network and use of ICT facilities

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

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

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

The effectiveness of any filtering and monitoring will be regularly reviewed.

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

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

6. PUPILS

6.1 Access to ICT facilities

- Computers and equipment in the trust's ICT suite and portable laptop trolleys are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used under the supervision of staff
- Sixth-form pupils can use the computers independently, for educational purposes only

6.2 Search and deletion

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 trust rules as a banned item for which a search can be carried out **and/or**
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos

- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher. 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.
- 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

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 'good reason' to do so.

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

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

If inappropriate material is found on the device, it is up to headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

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

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy / searches and confiscation policy

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

6.3 Unacceptable use of ICT and the internet outside of trust

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

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the trust's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the trust, or risks bringing the trust into disrepute
- Sharing confidential information about the trust, other pupils, or other members of the trust community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the trust's ICT facilities
- Causing intentional damage to the trust's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language

7. PARENTS

7.1 Access to ICT facilities and materials

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

However, parents working for, or with, the trust in an official capacity (for instance, as 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 are granted access in this way, they must abide by this policy as it applies to staff.

8. DATA SECURITY

The trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies.

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

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

- Data Backup

8.1 Passwords

All users of the trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

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

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

8.2 Software updates, firewalls and anti-virus software

All of the trust's ICT devices that support software updates, security updates and anti-virus products will have these installed, and be configured to perform such updates regularly or automatically.

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

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

8.3 Data protection

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

8.4 Access to facilities and materials

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

These access rights are managed by the Strategic ICT Network & Systems Manager

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 IT support team 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 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 Strategic ICT Network & Systems Manager

9. PROTECTION FROM CYBER ATTACKS

The trust will:

- Work with governors and the IT department 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), 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 once a day and store these backups on cloud-based backup systems that aren't connected to the trust network and which are stored off the trust premises
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider
    - 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
- Have a firewall in place that is switched on
- Develop, review and test an incident response plan with the IT department including, for example, how the trust will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. INTERNET ACCESS

The trust's wireless internet connection is secure.

- Internet access is filtered in the same way as all School internet traffic
- you have separate connections for
    - school devices
    - sixth form BYOD
    - guests

10.1 Parents and visitors

Parents 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 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 headteachers and Strategic ICT Network & Systems Manager 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 governing board is responsible for approving this policy.

Appendix 3: Acceptable use agreement for older pupils

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

Appendix 4: Acceptable use agreement for younger pupils

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

Appendix 5: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the trust's ICT facilities and the internet: agreement for staff, 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 inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the trust's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the trust's network • Share my password with others or log in to the trust's network using someone else's details • Share confidential information about the trust, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the trust	
I understand that the trust will monitor the websites I visit and my use of the trust's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside trust, and keep all data securely stored in accordance with this policy and the trust's data protection policy. I will let the 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:**