MOWBRAY
Education Trust

ICT and Internet Acceptable Use Policy

March 2023

Document Type	Published online and available to all staff
Last Revision Date	March 2023
Next Revision Date	March 2025
Owner	Trust IT Services Manager
Author	Trust IT Services Manager
Version	4.0
Status	

Contents

This policy applies to:

All Trust settings.

Where this policy states 'school' this means any of our educational establishments and the wider Trust.

Where this policy states 'Headteacher' this also includes 'Head of School' and 'Centre Manager.'

Mowbray Education Trust (MET).

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governance volunteers, volunteers, and visitors. It supports teaching and learning, pastoral, and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety, and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for users.
- Establish clear expectations for the way all users engage with each other online.
- Support the school's policy on data protection, online safety and safeguarding.
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT facilities.
- Support the school in teaching pupils safe and effective internet and ICT use.

This policy covers all users, including but not limited to governance volunteers, staff, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under the Mowbray Education Trust's Conduct and Disciplinary Policy and in some cases criminal proceedings.

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The General Data Protection Regulation
- 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
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2018
- Searching, screening and confiscation: advice for schools

3. Definitions

- **“ICT facilities**”: includes 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 ICT service.

- “**Users**”: anyone authorised by the school to use the ICT facilities, including governance volunteers, staff, pupils, volunteers, contractors and visitors.

- “**Personal use**”: any use or activity not related to the users’ employment, study or purpose.

- “**Authorised personnel**”: employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.

- “**Materials**”: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

4. Responsibility and Accountability

The Trust Board

4.1. Monitoring this policy and holding the Headteacher to account for its implementation.

4.2. Should ensure that they are familiar with the contents of this policy and its relationship to the school’s standards, policies, and guidance on the acceptable use of ICT and e-safety.

Headteacher

4.3. Ensure that all users are trained and become familiar with this policy and its relationship to the school’s standards, policies, and guidance on the acceptable use of ICT and e-safety.

4.4. Provide opportunities to discuss appropriate ICT and internet use on a regular basis and ensure that any queries raised are resolved swiftly.

4.5. Must ensure that any allegations raised in respect of ICT and internet use are investigated promptly and appropriately, in accordance with the school’s disciplinary procedure, code of conduct and acceptable use policy.

4.6. Must ensure two authorised personnel oversee each ICT and internet service.

Users

4.7. Should ensure that they are familiar with the contents of this policy and its relationship to the school’s standards, policies, and guidance on the acceptable use of ICT and e-safety.

4.8. Raise any queries or areas of concern they have relating to the use of ICT, the internet and interpretation of this policy with their Headteacher.

4.9. Must comply with this policy where specific activities or conduct is prohibited.

5. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities, by any user.

Unacceptable use of the school's ICT facilities includes:

5.1 Using the school's ICT facilities to breach intellectual property rights or copyright.

5.2 Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.

5.3 Breaching the school's policies or procedures.

5.4 Any illegal conduct, or statements which are deemed to be advocating illegal activity.

5.5 Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate.

5.6 Activity which defames or disparages the school, or risks bringing the school into disrepute.

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

5.8 Connecting any device to the school's ICT network without approval from authorised personnel.

5.9 Setting up any software, applications, or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts, or data.

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

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

5.12 Causing intentional damage to ICT facilities.

5.13 Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel.

5.14 Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.

5.15 Using inappropriate or offensive language.

5.16 Promoting a private business, unless that business is related to the school.

5.17 Using websites or mechanisms to bypass the school's filtering mechanisms.

This is not an exhaustive list. The school reserves the right to amend this list at any time. The headteacher and CEO will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Exceptions from unacceptable use

5.18 Where the use of school ICT facilities 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.

In such cases permission for any such activity would have to be sought prior to use by the headteacher. A risk assessment will be completed as appropriate.

Sanctions

5.19 Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on code of conduct.

See Behaviour Policy and Disciplinary Procedure.

6. Staff (including governance volunteer, volunteers, and contractors)

Access to school ICT facilities and materials

6.1. The school's IT department manages access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

- Computers, tablets, and other devices
- Access permissions for certain programmes or files

6.2. Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

6.3. Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the IT Department.

Mobile phones and e-mail

6.4. The school can provide a mobile phone for roles which require, this is at the discretion of the Headteacher.

6.5. School phones must not be used for personal matters unless prior arranged with your Headteacher.

6.6. Staff who are provided with mobile phones as equipment for their role must abide by this and all other relevant policies.

6.7. All school-related business should be conducted using the email address the school has provided.

6.8. School email accounts should be used for work purposes only.

6.9. BCC should be used when emailing groups.

6.10. Any attachments containing personal data must be password protected or encrypted, where possible, with the password emailed separately to the original email.

6.11. 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.

6.12. 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.

6.13. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 and The General Data Protection Regulation, 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.

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

6.15. 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 or disclose the information.

6.16. If staff send an email in error which contains the personal information of another person, they must inform the GDPR Officer immediately and follow our data breach procedure.

6.17. Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

Personal use and personal devices

6.16 Staff are permitted to occasionally use school ICT facilities and personal devices providing:

- It does not interfere with their jobs or prevent other staff or pupils from using the facilities for work or educational purposes.
- Does not take place during contact time.
- Does not constitute 'unacceptable use'.
- Takes place when no pupils are present.

6.17 The IT Department and headteacher may withdraw permission for it at any time or restrict access at their discretion.

6.18 Staff may not use the school's ICT facilities to store personal non-work-related information or materials.

6.19 Staff should be aware that use of the school's ICT facilities for personal use may put personal communications within the scope of the school's ICT monitoring. Where breaches of this policy are found, disciplinary action may be taken.

6.20 Staff are permitted to use their personal devices (such as mobile phones or tablets) in line with the school's Child Protection policy.

6.21 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 could see them.

6.22 Staff should take care to follow the school's guidelines on social media and the use of to protect themselves online and avoid compromising their professional integrity.

7. Social Media

Guidelines includes but is not limited to:

7.1. Users must not place any another user(s) at risk of harm and report any situation they come across which may contravene this.

7.2. Users must always follow statutory and school safeguarding procedures when using social media and report all situations that may contravene these procedures.

7.3. Social media and the use of must not be excessive and/or affect your ability to complete your duties.

7.4. If you are unsure of social media relationships, they must be declared with other personal relationships or interests whenever necessary or appropriate.

7.5. Users must maintain the reputation of the school, other users, and the wider community always and report any situation they come across which may contravene this – including but not limited to:

Contributing or access at any time, content including but not limited to illegal, discriminatory, sexual, or otherwise offensive content.

Using inappropriate language.

Using social media to criticise or insult.

Using social media to harass, bully or intimidate.

Using social media to breach school confidentiality.

Using social media to raise concerns about a school and/or users.

7.6. Staff should ensure that usage follows the guidelines set out in the Social Media policy. Breaches of this policy may be dealt with under the Mowbray Education Trust's Conduct and Disciplinary Policy and in some cases criminal proceedings.

8. Monitoring of school network and use of ICT facilities

8.1. The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

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

8.3. The school 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.

9. Remote Learning

9.1. Remote learning will only take place on platforms which have been assessed and approved by the school.

9.2. Only stakeholders within the Trust will be given access to Remote Learning platforms.

9.3. Staff will only use school managed accounts with learners and parents/carers.

9.4. Use of any personal accounts to communicate with learners and parents/carers is not permitted. Any pre-existing relationships or situations which mean this cannot be complied with will be disclosed to the Headteacher.

9.5. Staff will use school provided equipment e.g., laptop, tablet or another mobile device. Where this is not possible, staff must disclose this to the Headteacher. Upon agreement, staff must log out of the learning platform and ensure the device is locked when not in use.

9.6. Live streamed remote learning sessions will only be held with approval and agreement from the Headteacher.

9.7. Alternative approaches access will be provided to those who do not have access, stock permitting e.g. – loan device

Session Management

9.8. Privacy, safety settings and restrictions will be used to manage access and interactions in accordance with guidance set out by the Headteacher and authorised personnel.

9.9. Live 1 to 1 sessions will only take place with approval from the headteacher.

9.10. All participants will be made aware of session recording.

9.11. Recordings will be accessible by all staff, retained and securely disposed of in accordance with related policies.

9.12. When live streaming with learners:

- Contact will be made via leaners' school managed account.
- Staff will mute/disable learners' videos and microphones and should only be enabled under staff control at specific times.

9.13. A pre-agreed invitation detailing the session expectations will be sent to invitees:

- Access links should not be made public or shared by participants.
- Learners should not forward or share access links.
- If learners/parents/carers believe a link should be shared with others, they will discuss this with the member of staff running the session first.
- Learners are encouraged to attend lessons in a shared/communal space or room with an open door and/or when appropriately supervised by a parent/carer or another appropriate adult.

Behaviour Expectations

9.14. Staff will model safe practice and moderate behaviour online during remote sessions as they would in the classroom and in accordance with any related policy.

9.15. Staff will remind attendees of behaviour expectations and reporting mechanisms at the start of the session.

9.16. Educational resources will be used or shared in line with our existing teaching and learning policies, taking licensing and copyright into account.

10. Pupils

Access to ICT facilities

10.1. Computers and equipment in schools are available to pupils only under the supervision of staff and when in open communal areas.

10.2. Specialist ICT equipment, such as, not limited to that used for music or design and technology must only be used under the supervision of staff.

Search and deletion

10.3. Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

10.4. Any images or any other data or items banned under school rules or legislation that are part of safeguarding investigations or disclosures will be treated as described in the MET Child Protection policy.

10.5. The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Unacceptable use of ICT and the internet outside of school

10.6. The school will sanction pupils, in line with the Behaviour Policy, E-Safety Policy and Anti-Bullying Policy if a pupil engages in any of the following, not limited to, at any time, including Remote Learning (even if they are not on school 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 school's policies or procedures.
- Any illegal conduct, or 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.
- Activity which defames or disparages the school, or risks bringing the school into disrepute.
- Sharing confidential information about the school, other pupils, or other members of the school 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 school's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.

11. Parents

Access to ICT facilities and materials

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

11.2. Parents 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.

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

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn how to communicate respectfully with, and about others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

12. Data Security

12.1. The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

13. Passwords

13.1. Password management is supervised by the Trust IT department.

13.2. All users of the school's ICT facilities should set strong and/or biometric passwords.

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

13.4. Members of staff or pupils who disclose account or password information may face disciplinary action.

13.5. Parents or volunteers who disclose account or password information may have their access rights revoked.

14. Software updates, firewalls, and anti-virus software

14.1. School ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

14.2. 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 school's ICT facilities.

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

15. Data protection

15.1. All personal data must be processed and stored in accordance with data protection regulations and the school's data protection policy.

15.2. Personal data used by staff and captured or delivered during remote learning will be processed and stored with appropriate consent and in accordance with our data protection policy.

15.3. Any attachments containing personal data must be password protected or encrypted, where possible, with the password emailed separately to the original email.

16. Access to facilities and materials

16.1. Access to School ICT facilities is managed by the Trust IT Department.

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

16.3. 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 Trust IT Department immediately.

16.4. Users should log out of systems and/or lock their equipment when they are not in use to avoid any unauthorised access.

16.5. Equipment and systems should always be logged out of and closed completely at the end of each working day.

17. Encryption

17.1. The school ensures that its devices and systems have an appropriate level of encryption.

17.2. Staff may only use personal devices (including computers and USB drives) to access school 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.

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

18. Internet access & Wi-Fi

18.1. All filtering and Wi-Fi arrangements are managed by the Trust IT Department or authorised personnel.

18.2. Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

18.3. If any breach of filtering is identified the IT department are to be contacted immediately.

Pupils

18.4. Pupils cannot request additional access for websites.

Parents and visitors

18.5. Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher and Trust IT Department.

18.6. The headteacher will only grant authorisation if:

- Parents or visitors are working with the school in an official capacity (e.g., as a volunteer or as a member of the PTA)
- Required 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)

19. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline and code of conduct
- Data protection
- Anti-Bullying
- Data Retention

Log of Changes to Document

Version	Date	Page	Change	Approver:
V2.0	Apr-20	All pages	New policy created for HR/Operations Director review approval – following changes. 4.2 – ref. to disciplinary procedure added 6.1 – ref. to school added 7.2 – ref to parents/pupils signing agreement removed but appendices 2 & 3 on agreements retained for potential use in future	HR/Operations Director
V2.0	Apr-20	All Pages	Approved.	CEO
V3.0	Mar 22		4.0 – responsibility and accountability added. 6.0 staff – mobile phones and email re-written for clarity. 6.0 staff – personal use re-written for clarity. 7.0 social media – re-written to reflect the social media Policy. 8.6 remote learning data protection – broken down and incorporate into pre-existing headings. 9.0 remote learning – re-written for clarity. 10.0 monitoring and review – removed, added into responsibilities. 15.0 Data protection – re-written to include remote learning. 18.0 Internet Access – renamed to include WIFI.	AFR
V4.0	Mar 23		Review frequency amended to 24 months. 6.0 staff – personal use re-written for clarity. 10.4 - added to clarify safeguarding procedures(if necessary) for files on personal devices	

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils.
6. Don't use social media sites during school hours.
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the school on your profile (e.g., by setting it as your workplace, or by 'checking in' at a school event).
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises 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 do to if…

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the headteacher about what's happening.

A parent adds you on social media

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

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

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

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our school.

The school uses the following channels:

- Teams
- Class DOJO
- Tapestry
- Email/text groups for parents (for school announcements and information)
- School Website

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, Class DOJO 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 if they aren't 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 other children's parents/carers
- I understand that if my child needs to bring a mobile phone to school because they walk to and from school on their own that the phone will be handed into the office at the beginning of the day and collected at the end of the day.

Signed:	**Date:**

Appendix 3: Acceptable use agreement for younger pupils

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

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get 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
- Share my password with others or log in using someone else's name or password
- Bully other people

If I have wearable technology such as Apple watches, android watches or FitBits I understand that usage must not contravene this acceptable use.

I understand that the school will check the websites I visit and how I use the school'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 school 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.

I will not bring a mobile phone to school unless I have been given permission to do so.

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 agreement for staff, governance volunteers, volunteers, and visitors

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

Name of staff member/governance volunteer/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 private businesses, unless that business is 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.

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 school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed (staff member/governance volunteer/volunteer/visitor):	**Date:**