



Acceptable Use of IT Policy and Agreements

Version	1.1
Release date	April 2026
Next review date	April 2027
Description of changes	Treat as new

Contents:

1. Defining the scope of this policy	2
2. Responsibilities	2

Acceptable Use of IT: KS3&4 Student Agreement:

1. Context	3
2. Appropriate use of equipment	3
3. Protecting yourself and others online	3
4. Confirmation of agreement	4

Acceptable Use of IT: KS2 Display/Poster: 5

Acceptable Use of IT: Staff Agreement:

1. Context	6
2. Appropriate use of equipment	6
3. Appropriate use of internet and communications	6
4. Confirmation of agreement	7

1. Defining the scope of this policy

Information and communications technology include all forms of computing, the internet, telecommunications, digital media and mobile phones. Kingfisher Schools Trust employees have clear responsibilities regarding the use of all ICT equipment and ICT facilities. We have a duty to ensure the online safety of all pupils/students within the Trust.

Any member of staff that uses illegal software or accesses inappropriate websites when at work, or anytime using school owned devices, will face disciplinary action.

We expect all staff, following support and guidance as required, to sign and date the Acceptable use of IT agreement and be fully aware of and implement the Online Safety Policy. All staff have the duty to report any misuse of ICT equipment or ICT facilities.

Student responsibilities under this policy are set in line with the curriculum, meaning that appropriate expectations are set by their age. These expectations are reflected in the two different policies depending on Key Stage.

Key Stage 1 students will verbally be made aware of the expectations around the use of technology, as for some students, this may be their first encounter of digital technology.

2. Responsibilities

The Trust Board has:

- Delegated powers and responsibilities to the Chief Executive Officer and headteachers to ensure all members of staff, pupils/students and other stakeholders are aware of and comply with this policy
- Responsibility for ensuring funding is in place to support this policy

The Chief Executive Officer and headteachers will:

- Ensure all Trust staff are aware of and comply with this policy
- Ensure all Trust staff sign and date the "Acceptable use of IT: Staff Agreement" following support and guidance as required.
- Ensure all pupils/students sign and date the "Acceptable Use of IT: Student Agreement" following support and guidance as required.

All staff will:

- Comply with all aspects of the "Acceptable use of IT: Staff Agreement"
- Sign and date the "Acceptable use of IT: Staff Agreement" following any support or guidance required.

All KS3 and 4 Students will:

- Comply with all aspects of the "Acceptable use of IT: KS3&4 Student Agreement".
- Sign and date the "Acceptable use of IT: KS3&4 Student Agreement" following any support or guidance required

All KS2 Students will:

- Read the KS2 Student Acceptable use of IT poster displayed with their devices.
- Raise any concerns they may have whilst using technology with a teacher.

All KS1 Students will:

- Be explained what constitutes acceptable use of technology.
- Be made aware of how to raise any concerns that may have when using technology.



Acceptable Use of IT: KS3&4 Student Agreement

1. Context

Computers and other IT devices are an excellent learning resource when used appropriately and the following conditions apply to the acceptable use by pupils/students of these resources in school, to support your learning.

School devices are provided and maintained for the benefit of all pupils/students, and you are encouraged to use and enjoy these resources, and to help to ensure they remain available to all. You are responsible for good behaviour with the resources and on the Internet, just as you are in a classroom or on a school corridor. Remember that access is a privilege, not a right, and inappropriate use could result in that privilege being withdrawn.

No pupil/student is permitted to use school IT equipment without the permission of a member of staff.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to the behaviour policy. Additional action may be taken by the school, where appropriate, police may be involved.

2. Appropriate use of equipment

Pupils/Students agree to the following rules regarding the use of equipment:

- Do not install, attempt to install or store programs of any type on school devices
- Damaging, disabling or otherwise harming the operation of school devices, or intentionally wasting resources puts your work and the work of others at risk, and is prohibited
- Only use School devices for educational purposes
- Do not bring in or use USB storage devices unless given permission to do so by a member of staff
- If given permission to bring your own device (laptops, phones, tablets etc.) to school, always scan the device with anti-virus software, and ensure it has been found to be clear of viruses, before connecting them to the school's network. If you not sure how to do this, speak to a member of IT Staff.
- Protect school devices from spillages by eating and drinking well away from ICT equipment. Food and drink is not permitted in ICT Suites.

3. Protecting yourself and others online

Pupils/Students agree to the following rules to protect themselves and their peers safe online:

Security:

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Never reveal your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the school devices; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage and activity will be treated like school lockers. Staff may review your files and communications to ensure that you are using the system responsibly. We use monitoring systems to check that use is appropriate.

Internet:

- You must access the Internet only for study or for school authorised/supervised activities.
- Only access suitable material: Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other pupils/students or staff. This includes abiding by copyright laws.
- Social media must not be used in school.
- People you contact on the Internet are not always who they seem. Never meet someone who you only know from the Internet or via email.

Email

- Be polite and appreciate that other users might have different views from your own.
- The use of strong language, swearing or aggressive behaviour is as anti-social and subject to the law on the Internet as it anywhere else.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on the school device.

If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of staff. The sending or receiving of an email containing content likely to be unsuitable for children or schools is strictly forbidden.

Social Media:

- All pupils/students and parents/carers must read and comply with the Trust's Social Media Policy.

AI:

- AI may be used as a part of the learning process, but must be used to facilitate learning, not to replace it. For example, it would be acceptable to ask AI to explain a scientific topic to you, to help you complete a worksheet yourself. It would not be acceptable to ask AI to answer the questions for you.
- You may not submit any AI generated work as your own.

4. Confirmation of agreement

Please sign and date below; to confirm you have read and understood this document and agree to use the school devices within these guidelines.

Student Name:		Student Signature	
Parent / Guardian Name:		Parent / Guardian Signature:	
Tutor Group:		Date:	

Acceptable Use of IT: KS2

Rules for using computers, tablets and laptops:

- Only use these devices if you have been given permission to do so by an adult.
- Treat school equipment with care, just as you would if it were your own
- Do not eat or drink whilst using technology
- Only use this equipment to complete schoolwork.
- Do not reveal personal information about yourself or others to anyone online
- Be respectful of others when using computers. Do not type anything you know would not be acceptable if said in the classroom.

If you have any concerns about anything that you see whilst using computer equipment, report it to a teacher.



Acceptable Use of IT: Staff Agreement

1. Context

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet may be denied and you could be subject to disciplinary action. Where appropriate, police may be involved or other legal action taken.

2. Appropriate use of equipment

Staff agree to the following rules regarding the use of equipment:

- Damaging, disabling, or otherwise harming the operation of the Trust's devices, or intentionally wasting resources, puts your work and the work of others at risk and is prohibited.
- The school's and/or Trust's devices must only be used for educational/work purposes.
- Do not use removable USB storage without the permission of the School's/Trust's IT department. If you are approved to use USB storage, it must be scanned for viruses prior to use. Sensitive data should not be stored on USB storage. If used, staff are responsible for the data on USB storage, and for keeping those devices secure.
- Instead of using USB storage, files should be stored using approved cloud services, currently either Office365 or Google Workspace.
- If bringing in your own devices (e.g. laptops, phones, tablet PCs, etc.), check them with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network. If you are not sure how to do this, seek advice from a member of IT Support.
- Protect the Trust's devices from spillages by eating or drinking well away from any equipment.

Security:

- Do not share passwords for logging in to Trust devices, Trust networks or work-related applications
- Do not use someone else's username or password to log in to Trust devices, Trust networks or work-related applications
- Do not allow colleagues or other individuals to use a Trust device while you are logged on
- To protect yourself and the systems, do not attempt to bypass or alter security settings which may put you, your work, or the work of others at risk.
- Respect confidentiality, always lock devices when left unattended.

3. Appropriate use of Internet and Communications

Internet:

- Only access suitable material relevant to your role within the Trust. Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the Trust, as well as students or staff. This includes abiding by copyright laws.
- The schools monitor the use of Trust devices by staff and pupils/students and uses a reputation checking tool to monitor internet references to the school. Even material which is immediately deleted may be picked up by our monitoring systems.

Email:

- Ensure all emails are polite, respectful and professional
- Never use swear words, strong or aggressive language in email or attached documents
- Be wary of unsolicited attachments, even from people you know. Save and scan any attachments before opening them. If you are not sure how to do this, seek advice from a member of IT Support. Attachments can contain viruses or other programs that could destroy all the files and software on your computer, including other computers on the Trust or school networks.
- If you receive an email or other electronic communication containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to the Online Safety Lead.
- The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- Please be mindful that emails sent from a school's address are the school's property. The content of those emails is searchable and subject to data protection legislation.

Social Media:

- All staff must read and comply with the Trust's Social Media Policy.

AI:

- AI may be used as a part of some work processes (e.g. for brainstorming, automating labour intensive data entry or researching a topic). Any AI generated documentation must be checked in full.
- Staff must be aware of the risks of asking AI to summarize documents or write them on their behalf. In many documents, such as this policy, the details are important and could be missed if oversimplified by AI.
- Under no circumstances, may staff enter identifiable information of any organisations or person into any AI system unless given permission by the Director of IT.

4. Confirmation of agreement

Please sign and date below; to confirm you have read and understood this document and agree to use the school devices within these guidelines. I have also been made aware of how to contact IT support and the Online Safety Lead within my workplace

Employee Name			
Employee Signature		Date:	