



## **ACCEPTABLE USE POLICY AND AGREEMENT FOR STUDENTS**

The use of the Trust's ICT resources and services is a facility granted to students at the Trust's discretion.

This Acceptable Use Policy is designed to ensure appropriate use of devices and the schools' networks as well as ensuring students can benefit from using the Trust systems.

Use of the Trust/School network constitutes agreement to comply with this policy.

These rules apply to a student's use of the Trust/School network, whether using school computers or devices or using their own devices as a method to log in. This also applies to accessing the Trust/School network off site.

Students are given a user account to enable them use of the network and by continuing to use the network, users must abide by the following:

### **Student Terms of Use**

- You are responsible for account access on the Trust/School network. Any unauthorised use of your account should be flagged to the Trust's IT team immediately.
- Use of the Trust/School network is regularly monitored by the Trust's IT team (which includes email access). The Trust will monitor any traffic over the Trust systems to prevent threats to the Trust/School's network.
- You must not use someone else's username to gain access to the network.
- You should not write down or share your password with anyone else.
- You are not permitted to share access details to the Trust/School's network or Wi-Fi passwords with anyone else.
- You must not attempt to circumvent security of any host, network or account, or penetrate security measures ("hacking") on or accessed through the Trust/School network.
- You must not probe, scan or test the vulnerability of the network or other networks.
- You must not try to install any software on Trust or School systems without permission from the IT team. If software is installed without permission, it may cause extensive damage to the IT systems and users could be held personally liable for any costs incurred in rectifying the damage.
- Any apps or software that are downloaded onto your personal device whilst using the Trust/School's network is done at your own risk and not with the approval of the Trust.
- You must not use the network or your own property to access or process inappropriate materials. This includes (but is not limited to) pornographic material, material which may be seen as violent, offensive or discriminatory, inappropriate text files, gambling, gaming, taking inappropriate photographs or use files dangerous to damage the integrity of the network.
- You must not transmit, re-transmit, publish or store material or messages on or through the Trust/School network which could be perceived as bullying, threatening, abusive, hateful, indecent, harassing, offensive, defamatory or defamatory.
- You must report any inappropriate messages or information immediately to the IT team. This report will help protect other pupils and you.
- You are not permitted to access the Trust/School network using your own personal device, unless the device has been deemed acceptable to use by the Trust's IT team.

- You must not record, video or take pictures of other students, staff or third parties whilst using school devices without express permission from a senior member of staff.
- Use of own devices is at the risk of the user. The Trust cannot accept responsibility for any loss, damage or costs incurred due to use, damage or loss whilst accessing the Trust/School's systems.
- Storage media such as USB sticks and hard drives are prohibited at the Trust.
- Any property owned by students such as mobile phones, Android devices and iPads may not be used to stream, download or watch videos.
- You may not access the internet except through the Trust/School network.
- You must be mindful of the information that you post/share/send online and how this may impact others i.e., you should be kind online.
- Microsoft TEAMS: Chat and sharing must be limited to schoolwork. Accessing or processing inappropriate materials is strictly prohibited. This includes (but is not limited to) pornographic material, material which may be seen as violent, offensive or discriminatory, inappropriate text files, gambling sites, and gaming platforms. Taking and sharing inappropriate photographs or using files that could damage the integrity of the network is forbidden. Any action intended to damage the reputation of the school or others is not permitted. Students must report any incidents involving such materials or actions to a member of staff immediately.
- Accessing the TEAMS account of another student or member of staff is strictly prohibited and may result in the rights to use TEAMS being limited or permanently withdrawn.

If a student or user account breaches the above rules, their account may be inspected and their access stopped. A breach may also put you at risk of suspension and/or exclusion.

Appendix A: Student Acceptable Use Guide to using school technology

**Last review date:** 12.03.25

**Person responsible:** Trust Director of Technology



## Appendix A: Student Acceptable Use Guide to using school technology



### STUDENT ACCEPTABLE USE GUIDE TO USING SCHOOL TECHNOLOGY

This guide explains how to use the school's computers, internet, and online tools properly.

By using the school network, you agree to follow these rules.

	 DO	 DO NOT
<b>YOUR ACCOUNT</b>	Protect your account like your personal ID.	Share your password with anyone.
	Report any unauthorized use immediately.	Use someone else's username.
	Log out when you finish using a computer.	Write down your password where others can see it.
		Share network or Wi-Fi passwords with others.
<b>NETWORK SECURITY</b>	Only use the internet through the school network.	Try to "hack" or bypass network security.
	Report any security concerns to the IT team.	Probe or test the vulnerability of the network.
	Follow staff instructions about network use.	Attempt to access restricted areas of the network.
<b>YOUR DEVICES</b>	Get IT approval before connecting your device to the network.	Connect unapproved personal devices to the network.
	Take responsibility for your own device's safety.	Use USB sticks or hard drives at school.
	Use devices for educational purposes.	Stream, download, or watch videos on personal devices connected to the network.
		Install software on school computers without permission.
<b>APPROPRIATE CONTENT</b>	Use the internet for appropriate educational purposes.	Access adult content, violent material, or offensive content.
	Be mindful of what you view and share online.	Visit gambling sites or gaming platforms.
	Report inappropriate content to IT team immediately.	Download files that could damage the network.
	Be kind and respectful in all online communications.	Send bullying, threatening, or offensive messages.
<b>PHOTOS &amp; VIDEOS</b>	Get permission from staff before taking photos or videos.	Take photos/videos of others without permission.
	Only use cameras for authorized school activities.	Share inappropriate photos or videos.
		Record staff or students without express permission.
<b>MICROSOFT TEAMS</b>	Use TEAMS only for schoolwork.	Access another person's TEAMS account.
	Keep chats and sharing limited to school topics.	Share inappropriate content on TEAMS.
	Report inappropriate incidents to staff.	Use TEAMS to damage the school's reputation.
<b>CONSEQUENCES</b>	Breaking these rules may result in: <ul style="list-style-type: none"> <li>• Your account being checked</li> <li>• Loss of computer privileges</li> <li>• Possible suspension or exclusion</li> </ul>	