

ICT Acceptable Use Agreement

Terms and Conditions of this Agreement

Information Communication Technology (ICT) is integral to the lives of young people in today's society, both within school and in their lives outside school. ICT provision offers powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. However, the use of ICT carries a responsibility too.

This Acceptable Use Agreement is intended to ensure:

- That students remain safe while using the internet and other communication technologies for educational, personal and recreational use.
- That school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

1. Personal Responsibility

As representatives of Bishop Stopford School, students accept personal responsibility for reporting any misuse of the network to a staff member. Misuse may come in many forms, but it is commonly viewed as any message(s) sent or received that indicate or suggest pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use of which may be likely to cause offence and attempts to disrupt or hack into the computer network.

2. Acceptable Use

The use of ICT must be in support of education and research in accordance with the educational goals and objectives of Bishop Stopford School. Students are personally responsible for this provision at all times when using any ICT resource.

Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.

Use for commercial activities by for-profit organisations or personal enterprise is not acceptable.

3. Network Etiquette and Privacy

Students are expected to abide by the generally accepted rules of network etiquette. These rules include, but are not limited to, the following:

- Never send or encourage others to send abusive messages. Respect the rights and beliefs of others.
- Students should remember that they are representatives of the school on a global public system. Students must never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.
- Students should not reveal their or anyone else's personal information to anyone, especially their home address, email addresses or personal telephone number.

Please Initial here: _____

- Students should not reveal their password to anyone or attempt to login in to the school's ICT systems as another user. If a student thinks someone has obtained their password, they should contact a member of ICT Support immediately.
- Electronic mail (e-mail) is not private and the school reserve the right to view messages sent from and to the schools email systems.
- Students should cite references for any facts presented and not copy other people's work and imply that it is their own (i.e. plagiarism). Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.
- Students should not use the network in any way that would disrupt use of the services by others.

4. School Laptops

Part of the schools ICT provision for students centres around laptops. Laptops are typically less robust than desktop computers and require greater care and looking after. With this in mind students should:

- Ensure that they sign out the laptop that they using for the lesson, noting the laptop number on the logging sheet.
- At the class teacher's discretion it may be necessary to borrow laptops from other parts of the school. In this event students should collect them from the nearest location with a normal expectation of one student carrying one laptop only.
- Laptops should be carried with the lid closed and held with both hands.
- Upon the end of the lesson students should log off / sign out of their account on the laptop, and should only then shut-down the device.
- Upon returning the laptop to the lap safe students must plug the laptop into the mains power supply to ensure it is adequately charged for the next user and then sign to say they have returned the laptop in good repair on the logging sheet.

In the same way as reporting any other faulty device, students should alert their class teacher to the fault so this can be addressed by the ICT Support Team.

5. Services

Bishop Stopford School makes no warranties of any kind whether expressed or implied, for the network service it is providing. Bishop Stopford School will not be responsible for any damages suffered whilst on this system. These damages include loss of data as a result of delays, non-deliveries, miss-deliveries or service interruptions caused by the system or elements of the system, errors or omissions. Use of any information obtained via the network or other information systems is at the students own risk. Bishop Stopford School specifically denies any responsibility for the accuracy of information obtained via its Internet services.

6. Security

If students identify a security problem, they should notify a member of ICT Support at once and never demonstrate the problem to another student. Any user identified as a security risk may be denied access to the system and be subject to disciplinary action.

7. Vandalism

Vandalism is defined as any malicious attempt to harm or destroy any equipment or data of another user or of any other networks that are connected to the system. This includes, but is not limited to, the uploading or creation of computer viruses and malware, the wilful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

Please Initial here: _____

The school reserves the right to charge users for the replacement of equipment that is knowingly damaged or harmed.

Please Initial here: _____

8. Online Ordering systems

It is strictly forbidden for students to use the Internet for ordering goods or services regardless of their nature. In addition it is also forbidden for students to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.

9. Electronic Mail

The school may provide students with access to Electronic mail (e-mail). The sending or receiving of any email, which contains any inappropriate material (see section 1 for what this constitutes) is strictly forbidden. Disciplinary action will be taken in all cases. It is also forbidden to send large volume emails (spamming) and creating distribution and mailing lists.

10. Non Educational Online Activity

Students are not permitted to access non educational games, media (e.g. YouTube) or chat services available online.

11. Executable, Music and Video Files

Students are strictly forbidden from introducing or attempting to introduce executable files (eg '.exe, .cmd, .bat, .bin') to the network as these can contain harmful viruses. This includes but is not limited to copying such files onto shared network drives, saving them on your Home Area and running them from a USB memory stick.

Students are strictly forbidden from introducing music and video files (e.g. '.mp3, .mp4, .mpeg, .wav, .avi'). These files in many cases are copyrighted and the copying onto shared network drives or storing on your Home Drive may breach their copyright.

12. Personal Devices and Bring Your Own Device (BYOD)

Bishop Stopford School offers a Bring Your Own Device (BYOD) policy for sixth form students only. Sixth formers are permitted to connect their personal devices to the Guest Wifi. Once accessing the school WiFi students are required to accept the terms of the AUP upon accessing it.

Students using personal devices both at home and in school should be aware that access to School resources such as Office 365, Teams, E-mail and Foldr is monitored, and access is strictly controlled.

13. Saving Work

Students must not use external media (e.g. USB memory drives and external hard disks) as their primary storage repository as it is not possible to recover lost or corrupted files. Students are advised to save all files to their One Drive where it is routinely backed up.

Consequences for Misuse/Disruption

- Access to the school network may be removed or restricted.
- Sanctions appropriate to any individual action, with reference to the school behaviour policy, the school exclusions policy and the discretion of the head teacher.

The School reserves the right to monitor, inspect, copy, and review a personally owned device or file when staff have a reasonable suspicion that a violation has occurred.

In serious cases the School reserves the right to contact external authorities for advice, investigation and prosecution.

Please Initial here: _____

Please Initial here: _____

Student / Pupil Acceptable Use Agreement Form

This form relates to the student Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read and understood to the rules included in the Acceptable Use Agreement.

If you do not sign and return this agreement, access may not be granted to school ICT systems.

Name of Student

Form

Signed

Date

Please Initial here: _____

Please Initial here: _____