Rugby Free Secondary School

ICT and Internet Acceptable Use Policy

Terms and Conditions of This Agreement

1. Personal Responsibility

As a representative of the Rugby Free Secondary School, I will 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 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 Rugby Free Secondary School. Students are personally responsible for this provision at all times when using any ICT resource.

Use of other networks or computing resources must comply with the rules appropriate to that network. (eg within other partners of the Sixth Form or when on work placement)

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 generally not acceptable.

3. Privileges

The use of the ICT is a privilege and inappropriate use can result in that privilege being withdrawn. Students will participate in a discussion with a member of staff as to proper behaviour and use of the facilities. Staff will rule upon inappropriate use and may deny, revoke or suspend usage.

4. 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:

BE POLITE. Never send or encourage others to send abusive messages. Respect the rights and beliefs of others

USE APPROPRIATE LANGUAGE. Remember that you are a representative of the School on a global public system. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden.

PRIVACY. Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or any other students.

PASSWORD. Do not reveal your password to anyone. If you think someone has obtained your password, contact a member of ICT Support immediately.

ELECTRONIC MAIL. Electronic mail (e-mail) is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to appropriate authorities.

REFERENCE WORK. Cite references for any facts that you present. Do not copy other people's work and imply that it is your own (ie plagiarism). Plagiarism leads to formal action, up to and including, withdrawal from examination and qualifications.

DISRUPTIONS. Do not use the network in any way that would disrupt use of the services by others.

5. Services

Rugby Free Secondary School makes no warranties of any kind whether expressed or implied, for the network service it is providing. Rugby Free Secondary 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, mis-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. Rugby Free Secondary School specifically denies any responsibility for the accuracy of information obtained via its Internet services.

6. Security

If you identify a security problem, notify a member of ICT Support at once. Never demonstrate the problem to another student. All use of the system must be under your own username and password. Remember to keep your password to yourself. Do not share it with friends. Anyone caught disclosing passwords may have their access denied and may be subject to disciplinary action. 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, the willful damage of computer hardware, whether connected to the network or not, the deletion of data from its place of storage.

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

Electronic mail (email) is provided by the School, the use of Internet based email systems is forbidden. The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden. This material includes, but is not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, any use which may be likely to cause offence. Disciplinary action will be taken in all cases. It is also forbidden to send large volume emails (spamming).

10. Non Educational Online Activity

Students are not permitted to access non educational games, media (eg YouTube) or chat services available online unless given access by a member of staff for strictly educational purposes only.

11. Internet Search Engines

Students are required to use Internet search engines responsibly. If students are found to be searching for material unsuitable and in breach of this policy they will face disciplinary action.

Students are strictly forbidden from removing safety filters from Internet Search engines in order to access unsuitable material. This includes but is not limited to the removal of the SafeSearch feature.

12. Executable, Music and Video Files

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

Students are strictly forbidden from introducing music and video files (eg '.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.

Students are strictly forbidden from downloading executable, music and video files when using the School's Internet provision.

13. Bring Your Own Device (BYOD)

Students choosing to connect their personal devices to the School's wireless network accept that, where appropriate, they must comply with the requirements and terms of this policy and abide by the guidelines described below.

14. Accessing Remote Systems

Students are only permitted to access remote systems authorised by Rugby Free Secondary School. These systems include, but are not limited to, those deployed by schools within the Trust.

15. Saving Your Work

Students must not use external media (eg USB memory 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 Home Drive where it is routinely backed up and easily accessed both onsite and remotely. Students are advised to regularly save amendments to their files to minimise data loss if their service is interrupted

Guidelines for Acceptable Use of Personal ICT Devices

- The use of personal ICT devices falls under the ICT and Internet Acceptable Use Policy which all students must agree to, and comply with.
- The primary purpose of the use of personal devices at a School site is **educational**. Using the device for personal reasons should only take place after permission has been given from a teacher or other member of staff. Students must use devices as directed by their teacher.
- Students must use their own network credentials to connect to the School's wireless network. Students shall make no attempts to circumvent the School's network security. This includes, but is not limited to, setting up proxies and downloading programs to bypass security.
- The use of a personal ICT device is not to be a distraction in any way to teachers or students. Personal devices must not disrupt lessons or private study areas in any way. Playing games or other non-educational work related activities are not permitted.
- Students are not permitted to use any electronic device to record audio or video media or take pictures of any student or staff member without their permission.
- Students shall not distribute pictures or video or any other material relating to students or staff without their permission (distribution can range from emailing/texting to one other person to posting images or videos online).
- Students are not to call, text message, email, or electronically communicate with others from their personal device, including other students, parents, guardians, friends, and family during lessons unless permission has been given from a teacher or other member of staff.
- Students are expected to act responsibly and thoughtfully when using technology resources. Students bear the burden of responsibility to inquire with ICT Support and/or teachers when they are unsure of the permissibility of a particular use of technology prior to engaging in the use.
- Students may not utilize any technology to harass, threaten, demean, humiliate, intimidate, embarrass, or annoy their classmates or others in their community. This is unacceptable behaviour known as cyber bullying and will not be tolerated. Any cyber bullying that is determined to disrupt the safety and/or wellbeing of the School will be subject to disciplinary action.
- Students must check their personal ICT device daily to ensure the device is free from unsuitable material and free from viruses etc. before bringing the device onto a School site.
- Students must check their personal ICT device daily for basic Health and Safety compliance to ensure it is free from defects. Any personal ICT device that has obvious Health and Safety defects should not be brought onto a School site.
- Students are responsible for charging their personal ICT devices prior to bringing them onto a School site. Personal ICT devices cannot be connected to School power outlets without first being PAT tested by one of the School's designated PAT testers.

Consequences for Misuse/Disruption

In addition to dealing with misuse/disruption within the remit of the School's ICT Acceptable Use Policy (AUP) and Behaviour Management Policy one or more of the following sanctions may apply:

- Personal ICT device may be confiscated and kept at the Main Office until a student's parent/guardian collects it.
- Privilege of using personal ICT devices may be removed.
- Access to the School's wireless network may be limited or withheld.

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.

Dated: 5 October 2017