The John Fisher School

ICT Acceptable Use Policy

Responsible: Governors' Resources Committee
Next Review Date: June 2021

Nurturing young Catholic gentlemen
Aspiring for Academic, Cultural & Sporting Excellence

The John Fisher School believes that online safety (e-Safety) is an essential element of safeguarding students and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles. All students must follow the conditions described in this policy when using School ICT networked resources including internet access, the school learning platform both in and outside of school. To qualify for network, internet and e-mail access, students must read, sign and return an agreement.

The John Fisher School strongly believes in the educational value of such electronic services and recognises their potential to support the curriculum. Every effort will be made to provide quality experiences for students and teachers using this information service. Inappropriate and/or illegal interaction with any information service is strictly prohibited.

If British decency laws are breached or the Computer Misuse Act 1990 is breached then a student is likely to have the matter referred to other authorities including the police. The Computer Misuse Act 1990 identifies three specific offences:

1. Unauthorised access to computer material (that is, a programme or data).
2. Unauthorised access to a computer system with intent to commit or facilitate the commission of a serious crime.
3. Unauthorised modification of computer material.

Please read this document carefully, only once it has been signed and returned will access to the computer system be permitted. Listed below are the provisions of this agreement. If any student violates these provisions, access to the network, internet and e-mail will be denied and the student will be subject to disciplinary action.

Terms and Conditions of This Agreement

1. Personal Responsibility

As a representative of The John Fisher 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 The John Fisher 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. (e.g. within other partners of the Joint 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 (i.e. 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

The John Fisher School makes no warranties of any kind whether expressed or implied, for the network service it is providing. The John Fisher 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 student's own risk. The John Fisher 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 wilful 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 (e.g. YouTube) or chat services available online.

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 Safe Search feature.

12. Executable, Music and Video Files

Students are strictly forbidden from introducing executable files (e.g. '.exe, .cmd, .bat, .bin') to the network as these can in 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 (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 Student Drive (H:\) may breach their copyright.

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

13. The Personal Laptop Use Agreement

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 School's Personal Laptop Use Agreement.

14. Accessing Remote Systems

Students are only permitted to access remote systems authorised by The John Fisher School.

15. Saving Your Work

Students must not use external media (e.g. 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 (H:\) 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.

16. Acceptable Use Policy for Staff Internet access.

Internet Access: Staff must not access, or attempt to access, websites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. It is recognised that under certain circumstances inadvertent access may happen. Should a member of staff or a student access any of these sites unintentionally they should report the matter to a member of the Senior Leadership Team so that it can be logged.

Inappropriate/Illegal content: Access to any of the following will be reported to the Police: images of child sexual abuse (sometimes incorrectly referred to as child pornography). These are images of students apparently under 16 years old or older involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

Social networks: Members of staff should never knowingly become "friends" with students on any social networking site or engage with students on internet chat.

Communication: All members of staff should use their school email address for conducting professional business. This includes communicating with parents/carers and students.

Remote Access: Staff are permitted access to their school documents using the secure remote desktop protocol (RDP). Please ensure full compliance with data protection and do not leave your home computer unattended when logged in.

Passwords: Keep your passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection: Where a member of staff has to take home sensitive or confidential information, sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted and does it have to be on a USB memory stick that can be easily misplaced? All data relating to staff, students and parents/carers must be kept private and confidential.

Personal Use: Staff are not permitted to use ICT equipment for personal use without Senior Leadership Team approval. If personal use is permitted the boundaries of use should be written down and adhered to.

Images and Videos: No images or videos should ever be uploaded to a website or social network without the express permission of parents or the student's carer. Similarly, no personal information (name, date/place of birth, mobile number, email address etc.) should ever be shared.

Use of Personal ICT devices: Use of personal ICT equipment (i.e. mobile phones, cameras, personal laptop etc.) is at the discretion of the Senior Leadership Team. Any such use should be stringently checked for up to date anti-virus and malware checkers. Use of personal ICT devices is subject to the same Acceptable Use Policy. Pictures or videos of students must never be taken using personal ICT devices.

Reporting concerns: It is the duty of staff to support the School's Child Protection and Safeguarding Policy and report any behaviour (staff or students), which is inappropriate or a cause for concern, to the Designated Safeguarding Lead.

Monitoring: Emails and internet activity are subject to monitoring. The Child Protection & Safeguarding Policy, which includes guidance on online safety, and the Staff Handbook contain a comprehensive overview of all ICT–related matters. Staff should read these carefully in order to be well-informed and compliant with all school policies.

http://fluencycontent2-schoolwebsite.netdna-ssl.com/FileCluster/TheJohnFisherSchool/MainFolder/our-school/policies/Child-Protection-and-Safeguarding-Policy.pdf

Appendix 1:

THE JOHN FISHER SCHOOL PERSONAL LAPTOP USE AGREEMENT FORM

Personal Use of Student-Owned Laptops in School

PURPOSE:

This policy is to allow students that have personally owned laptops the ability to access the school's wireless network as a means of enhancing the students' educational experience. Permission to bring and use a personal laptop is contingent upon adherence to the School's internet policy as well as the following conditions. General Use Conditions: The John Fisher School provides the opportunity for students to bring a personal laptop to school to use as an educational tool under the following conditions:

1. The school's written confirmation or permission is necessary for student use of a personal laptop in the classroom or on the school premises. Teacher discretion may also dictate use for only specific activities, such as internet access, word processing or note taking.

2. When not in use or required for any lesson or activity, students must turn off and put away their personal laptop as requested by a teacher or Learning Support Assistant.

3. The use of the laptop is solely limited to support the educational activities occurring within the classroom and where necessary to complete work outside of the classroom.

4. All sound must be muted. Exceptions may be granted by the teacher, such as the use of sound associated with the instructional activities, or the use of headphones.

5. The personal laptop owner is the only person allowed to use the laptop.

6. Students may use their personal laptop in adult supervised areas only, such as the classroom, library or other areas where a teacher or other member of staff is present. The laptop should be used for educational purposes during these times; playing games or other non-instructional activities is prohibited.

7. Failure to comply with these guidelines may result in confiscation of the laptop for the remainder of the day and/or loss of laptop use privileges.

8. An updated **Anti-Virus software must** be on the laptop in order to gain access to the school's network.

9. Access to the wireless network will be granted only upon return of this form and approval of the Headteacher.

Laptop Security

Be aware that laptops and other portable electronic devices are especially vulnerable to loss and theft; students should secure these items when not in use, and never leave an unsecured laptop unattended. Students who bring personally owned items on school property must assume total responsibility of these items. The John Fisher School will not accept responsibility for loss, damage, theft of personally owned laptops brought onto school property. Laptops and all other portable or digital electronic items that are lost, stolen or damaged are the responsibility of the student and their parents or carers. It will not be the schools responsibility to search for or replace a personal laptop which is lost or stolen. The school Network Manager or IT Technician cannot attempt to repair, correct, or be responsible for malfunctioning personal hardware or software. The Network Manager or IT Technician may examine the laptop and search its contents if there is reason to believe school policies or guidelines have been violated. Depending on the violation, the confiscated device may be turned over to local law enforcement and legal action may occur in accordance with the law.

The John Fisher – Personal Laptop Use Policy Parent/Carer and Student Agreement

I have read The John Fisher Personal Laptop Policy and understand the conditions for use of a personal laptop on school property. I understand that violation of these provisions could result in the confiscation of a personal laptop or other portable electronic device by the school administration or local law enforcement, and that legal action may be used in accordance with the law. I assume total responsibility for loss, damage or theft of a personal laptop brought onto school grounds.

I give my permission for my son, (please print name) _____ to use a personally owned computer on the wireless network at The John Fisher School.

Parent/Carer signature_____Date_____
Student signature_____ Date_____
Laptop/netbook brand_____

Identifying serial number_____

Colour _____

Please refer to The John Fisher 'Responsible Computer/Internet Use' Agreement, and the 'ICT Acceptable Use' Policy in student's planner.