St. Philip Howard
Catholic Voluntary Academy

ACCEPTABLE USE OF ICT POLICY

2017/2018

Students

Lead	Louisa Morris
Policy Status: Approved/Awaiting Approval	Approved Summer 2017
Prepared by:	Mike Kays
Next Review:	Summer Term 2018
This Version No.	1

Valid only at the time of issue

All users must read this Acceptable Use Policy then sign and return the attached agreement to the ICT Network Manager who will keep it on file.

The staff at St Philip Howard Catholic School believe in the educational value of the internet and other ICT services and recognise their potential to support the curriculum. Every effort will be made to provide quality experiences to students and staff using this information service. However, inappropriate and/or illegal interaction with any information service is strictly prohibited. Monitoring software is in use on the school network.

Responsibilities

The use of electronic services must be in support of education and research in accordance with the educational goals and objectives of St Philip Howard School. Users are personally responsible for this provision at all times when using any ICT equipment or electronic information service provided by the school. Transmission or use 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.

Network Etiquette and Privacy

You 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.
- 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.
- Respect Privacy. Do not reveal any personal information to anyone, especially the home address or personal telephone of yourself or others.
- Password. Do not reveal your password to anyone. If you think someone knows your password, change it.
- Malware. Don’t distribute viruses or other malicious software.

- E-Mail. Electronic mail is not guaranteed to be private. Messages relating to, or in support of, illegal activities may be reported to the authorities. Do not send spam emails.
- Disruptions. Do not use the network in any way that would disrupt use of the services by others.
- Illegal activities. Illegal activities of any kind are strictly forbidden.
- Internet shopping. It is forbidden to use internet shopping websites including Ebay, as this is inappropriate use of the system.
- Chat Services. Students may not use internet chat sites or software, and staff may only use it in support of the teaching and learning objectives for the students (remember you are an ambassador of the school).
- Social Networking Websites – Staff and Students may not use these sites on school equipment. The school has provided a VLE which can be used in the same way as many social networking sites.
- Games – students and staff are not allowed to play games on the schools ICT equipment, except where this is in direct support of a learning objective for a student or group of students and even then only from a pre approved list.

Security

Security is everyone's responsibility.

Access to the network is controlled via a unique username and password, All users should ensure that their password is kept secret, as this will allow access to their documents and other resources on the network. Always use complex passwords with uppercase, lowercase and numbers. Never use the same password for different systems (if it is compromised then all systems are compromised). Anyone attempting to use a username and password which is not their own is breaking the law under the computer misuse act 1990 and could face legal consequences.

Log off the computers when you are no longer using them, if you are in the middle of something then you can lock the computer by pressing CTRL-ALT-DEL and choosing Lock Computer, this will leave programs running in the background but prevents unauthorised access. Students are not allowed to use staff laptops even if they login as themselves.
Physical security is the first line of defence, doors to rooms that have computers in them must be locked when they are not in use.

Ownership of equipment

All ICT assets belong to the school, including laptops issued to individuals. This means that they may only be used for school related purposes. Activity logs are kept and these may be used to investigate misuse of school ICT resources.

Inappropriate use of school resources includes, but is not limited to

- They must not be used to store personal documents and data. (including Photos and Music)
- The individual may not allow the equipment they have been issued to be used by anyone else.
- Must not be used in connection with any other business.
- Must not be used for any illegal activities (equipment can be seized by law enforcement agencies)
- Must not be used to buy and sell on any online websites.

Social Networking Websites

Staff and Students may not use these sites on school equipment. This applies to all Social networking sites, for example Facebook, Bebo, My Space.

Installing Software

Students and staff are not allowed to bring private software disks into school. This policy is designed not only to ensure that the school is not in breach of copyright laws but also to reduce the risk of Viruses, Trojans, Worms, Malware, Adware and other undesirable software. Some legitimate software may also cause problems if it conflicts with existing software or settings already installed. Students may provide their own 'work disks' but these must not be used to store software, inappropriate material, or anything that is subject to copyright restrictions.

Internet

The use of the Internet and other electronic services is a privilege and inappropriate use will result in that privilege being withdrawn.
Students are not allowed to access the Internet or any other external communications system unless they are supervised by a member of staff and the school has received the students acceptable use policy signed by them and by their parent/guardian. Attempting to bypass any of the internet filters is in breach of the computer misuse act 1990 and will lead to loss of privilege, and may lead to disciplinary or legal consequences.

Inappropriate material

School is naturally concerned about all forms of computer misuse but the greatest threat to our students' well being is from inappropriate content and since we have a duty of care, we must obviously take steps to counter this threat.

In order to protect our students from the dangers of such material, the following actions will be taken

- Students should not bring CD ROMs or floppy disks (or any other removable media) to school except where they have express permission and it contains only documents that are to be used in direct support of a lesson being studied. These work disks will be inspected at random.

- Students will not be allowed to use computers unless properly supervised by teaching staff.

- The school will only allow access to the Internet through approved 'service providers', with filtered Internet feeds, but it must be noted that these are not 100% effective and some inappropriate material may get through. Staff should speak to the students about acceptable use, and if it happens again internet access will be removed for that student.

- The school ICT Support Department operates a system of random checks on user's home areas on the school servers and internet history on school computers. Any inappropriate material found in this way will be deemed to be serious misuse and will result in withdrawal of access and other appropriate action.

- School uses monitoring software to ensure that users are complying with this policy.

Equipment misuse

During lessons in which computers are used staff will be watching for any attempts to wilfully damage computers. All damage however small must be reported to the ICT Manager immediately including the name of anyone found to be responsible.

Malicious attempts to harm or destroy any equipment or data including, 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 other users or shared data from its place of storage. Damage to equipment and data reduces the service availability to all users and adversely affects lessons and will not be tolerated. A member of the Senior Management Team will follow up any incidents. The school reserves the right to charge for damage where appropriate.

Electronic mail

The sending or receiving of any email, which contains any inappropriate material, is strictly forbidden as is sending large volume Emails (Spamming).

Other common email attacks you should be aware of are:-

- Viruses and Malware are often spread by emails that tell you to “forward this onto everyone in your inbox” or say things like “this is not a hoax”.

- Phishing attacks are emails pretending to be from a reputable source, when in fact they are trying to trick you into giving out personal information. They may appear to be from a bank or similar company but often use strange terminology and just sound suspicious.

- Some attachments can contain viruses and malware, so be suspicious if you have not requested to be sent the attachment.

Food and Drink

Absolutely no food in the ICT classrooms. Drinks limited to water - in line with school policy students may drink water in lessons, but water to be drunk away from the machines and no drink bottles placed on computer benches even if the drink and computer are not in use.

Under no circumstances should fizzy pop even be seen near a computer.

St Philip Howard ICT Acceptable Use Policy for Students

REQUIRED SIGNATURES

I understand and will abide by the provisions and conditions of this agreement. I understand that any violations of the above provisions may result in disciplinary or legal consequences and the revocation of my privileges. I also agree to report any misuse of the system to a Teacher or member of the ICT Support Team.

Name Parent/Carer Name

Signature Parent/Carer Signature

Date Date