ST. ILLTYD'S CATHOLIC HIGH SCHOOL

ICT Acceptable Use Policy - Staff

Sept 2023

ICT resources and Internet access are available to all staff in the school. All users are required to follow the conditions laid down in the policy. Any breach of these conditions may lead to withdrawal of the user's access, monitoring and or retrospective investigation of the users use of services, and in some instances could lead to criminal prosecution. Any breach of the conditions will also be considered a disciplinary matter.

These resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. Any use of the network that would bring the name of the school or County Council into disrepute is not allowed.

The school expects that staff will use these technologies as appropriate within the curriculum and that staff will provide guidance and instruction to pupils in the use of such resources. Pupils accessing school ICT resources must be supervised at all times. All computer systems will be monitored to ensure that they are being used in a responsible fashion.

The term ICT resources includes data and data storage, online and offline communication technologies and access devices. Examples include laptop PCs, desktop PCs, mobile phones, tablets, digital cameras, cloud-hosted systems (ie those that the school uses via the internet) and email.

ACCEPTABLE USE - STAFF

It is the responsibility of all staff accessing school ICT resources to take all reasonable steps to ensure compliance with the conditions set out in this Policy document, and to ensure that unacceptable use of the school ICT provisions does not occur. Users must comply with the acceptable use policy of any other networks that they access. This is vital in order to ensure the security of our network and the integrity of the data we keep regarding our students, in compliance with the Data Protection Act (1998).

Users are expected to utilise the network systems in a responsible manner. The following points are to be adhered to in order to comply with both the school's ICT and Data Protection Policies.

1. Do not reveal any of your passwords to anyone. If you think someone knows one of your passwords, report the incident to ICT Support and change it as soon as possible. If this is not possible, contact the ICT Support department who will change it for you.

2. Passwords for staff accounts must not be written anywhere that may be visible to pupils.

3. Staff passwords must meet the minimum complexity requirements and be changed every 90 days.

4. Staff are to always use their own user account when accessing the school network and SIMS.net.

5. Electronic mail may be monitored. The Head teacher reserves the right to authorise investigations into unauthorised activity using the school's email systems.

6. Personal email accounts are not to be used for any school purposes.

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

8. Any unsuitable websites accessed via through the school network should be reported to the ICT Support department immediately.

9. Any external storage device brought from outside of school must be checked for viruses prior to use with school devices.

10. Internet Access is monitored by Cardiff Council ICT department at all times. Any attempt to circumvent the school's web filter will result in suspended access and disciplinary.

11. All software must be verified by the ICT Support department before use on school devices.

12. Files and folders stored on the school network may be accessed by the ICT department at any time.

13. Staff are to report any issues, damage or errors with school ICT equipment to the ICT Support department as soon as is possible to do so after discovering the issue.

14. Files containing personal or sensitive data must be stored appropriately in accordance with the Data Protection policy.

Network Security

Users are expected to inform the ICT Support department immediately if a security problem is identified. Do not demonstrate this problem to other users. Users identified as a security risk will be denied access to the network.

Physical Security

Staff users are expected to ensure that portable ICT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Items that need to be left over breaks and lunchtimes for example will need to be physically protected by locks and or alarms.

Wilful Damage

Any malicious attempt to harm or destroy any equipment or data of another user or network connected to the school system will result in loss of access, disciplinary action and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of

Data Storage

Any file that contains any information that can be used to identify an individual is classed as personal data. This data must be treated in accordance to the school's data protection policy. Do not take anything containing personal data off site unless it is on an encrypted drive. If you are not sure – consult with the IT department or the School Business manager. This includes sharing documents from Office 365 with third parties or personal email addresses.

All school documents should be stored on one of the available network drives (eg user documents folders, shared areas) or in our Office 365 tenancy. The school cannot be held responsible for loss of data stored in other locations.

Communication Expectations

All staff are provided with a cloud hosted email solution, to which 24/7 access is provided via the internet. Though staff are free to send email whenever is convenient for them, there is no expectation on staff to monitor or respond to email outside of their contracted school hours.

E-Safety

Staff have the following responsibilities in line with the school's approach to safeguarding students using internet access:

• They have an up to date awareness of e-Safety matters and of the current school e-Safety policy and practices

• They have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP / AUA)

• They report any suspected misuse or problem are escalated to the relevant team for investigation / action

• All digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems

• E-Safety issues are embedded in all aspects of the curriculum and other activities

• To ensure students understand and follow the e-Safety and acceptable use policy

• To ensure students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

• To monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices

• In lessons where internet use is pre-planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Services

There will be no warranties of any kind, whether expressed or implied, for the network service offered by the school. The school will not be responsible for any damages suffered while on the system. These damages include loss of data as a result of delays, non-deliveries, or service interruptions caused by the system or your errors or omissions. Use of any information obtained via the network is at your own risk. Using software from unauthorised sources is prohibited.