St. Paul’s Catholic School

ICT Acceptable Use Policy

Networked resources, including Internet access, are available to pupils and staff in the school. All users are required to follow the conditions laid down in this policy. Any breach of these conditions may lead to withdrawal of the user’s access and be treated as a disciplinary matter.

Our networked resources are intended for educational purposes, and may only be used for legal activities consistent with the rules of the school. The school expects that pupils and staff will use new technologies as appropriate within the curriculum. All computer systems will be regularly monitored to ensure that they are being used in a responsible fashion.

CONDITIONS OF USE

Personal Responsibility

Access to the networked resources is a privilege, not a right. Users are responsible for their behaviour and communications. Staff and pupils will be expected to use the resources for the purposes for which they are made available. Users will accept personal responsibility for reporting any misuse of the network to the ICT Manager.

Acceptable Use

Users are expected to utilise the network, email and internet systems in a responsible manner. ICT is constantly changing, at this moment in time the following list provides some guidelines on the matter:

NETWORK ETIQUETTE AND PRIVACY

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

1. Be polite – never send or encourage others to send abusive messages.
2. Use appropriate language – users should remember that they are representatives of the school on a global public system. Illegal activities of any kind are strictly forbidden.
3. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
4. Privacy – do not reveal any personal information (e.g. home address, telephone number) about yourself or other users. Do not trespass into other users’ files or folders.
5. Password – do not reveal your password to anyone. If you think someone has learned your password then contact ICT department.
6. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported.
7. Disruptions – do not use the network in any way that would disrupt use of the network by others.
8. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.

9. Staff or pupils finding unsuitable websites through the school network should report the web address to the ICT Manager.
10. Do not copy programme files which exceed 100MB, video or.music files from media devices such as “pen drives” into the network.
11. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity, sites visited are monitored).
12. Do not download material that is illegal onto the school network. Copyright laws must be abided by.
13. Unapproved system utilities and executable files will not be allowed in pupils’ work areas or attached to e-mail.
14. Files held on the school’s network will be regularly checked by the ICT Department.
15. It is the responsibility of the User (where appropriate) 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 Internet/Intranet does not occur.

ACCEPTABLE USE

Examples of acceptable use include but are not limited to the following:

- Users must login with their own user ID and password, where applicable, and must not share this information with other users. They must also log off after their session has finished.
- Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.

UNACCEPTABLE USE

Examples of unacceptable use include but are not limited to the following:

- Accessing or creating, transmitting, displaying or publishing any material (e.g. images, sounds or data) that is likely to cause offence, inconvenience or needless anxiety. (The school has filters in place to block e-mails containing language that is or may be deemed to be offensive.)
- Accessing or creating, transmitting or publishing any defamatory material.
- Receiving, sending or publishing material that violates copyright law.
- Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
- Transmitting unsolicited material to other users (including those on other networks).
- Unauthorised access to data and resources on the school network system or other systems.
- User action that would cause corruption or destruction of other users’ data, or violate the privacy of other users, or intentionally waste time or resources on the network or elsewhere.

Social Networking Site

Social networking sites such as MySpace and Facebook are blocked by the school filter. However, the school realizes many pupils and staff have access to these sites outside of school. Pupils and staff are reminded that regardless of where their posting originates, any posting of photographs, text or videos to these or similar sites which can be considered as being derogatory to the school, the school community, or be threatening, demeaning, or a form of bullying to either staff or student, may result in action being taken by the school on the person who posted the comment or material.

Email Protocol

Communications by e-mail should consist of information sharing or positive feedback. If staff wish to raise a concern, make a complaint or convey a criticism this should always be done face to face or as appropriate, with the support of a line manager.

Additional guidelines

- Users must not download software without approval from the ICT Manager.
- Auditing software on the network tracks usage of computers by username; therefore if a username and password has been used it will be assumed to have been used by the owner and therefore any consequences will devolve upon that owner.
- It is good practice to password protect the machine when it is not in use.

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.

NETWORK SECURITY

Users are expected to inform the ICT Manager immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user ID and password, where applicable, and must not share this information with other users. Users identified as a security risk will be denied access to the network.

PHYSICAL SECURITY

All 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.

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 and if applicable, disciplinary action. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

MEDIA PUBLICATIONS

Named images of pupils (e.g. photographs, videos, web pages etc.) must not be published under any circumstances. Written permission from parents or carers will be obtained before photographs of pupils are published on the school web site.

SUPERVISION AND MONITORING

School and network administrators and their authorised employees monitor the use of information technology resources that help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the school's information networks in order to further the health, safety, discipline, or security of any student or other person, or to protect property. Teachers or relevant employees reserve the right to access pupils' accounts for monitoring and marking of pupils' work.

DISCLAIMER

St Paul's will supervise pupils and take all reasonable precautions to ensure that users access only appropriate material. We will provide a filtered internet service using a combination of approaches. No system however can be completely effective and we rely on staff and pupils taking personal responsibility and working with the school, governors and parents to ensure every reasonable measure has been taken.