ST WILFRID'S CATHOLIC SCHOOL

DIGITAL & ELEARNING POLICY

"To equip his people for works of service, so that the body of Christ may be built up"
[Ephesians 4: 12]

1. AIM

To promote learning through the use of technology and provide guidelines for its use.

2. POLICY CONTENTS

a. Acceptable Use Policy (Students & Staff)
b. BYOD Policy

3. CONDITIONS OF USE

a. 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 are to take due care with the physical security of hardware they are using. Users will accept personal responsibility for reporting any misuse of the network to the IT Helpdesk.
b. Acceptable Use - Users are expected to utilise the network systems in a responsible manner. It is not possible to set hard and fast rules about what is and what is not acceptable but the following list provides some guidelines on the matter:

4. 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:

a. Be polite – never send or encourage others to send abusive messages.
b. 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.
c. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority group.
d. 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.
e. Password – do not reveal your password to anyone. If you think someone has learned your password then contact the IT Helpdesk.
f. Electronic mail – Is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Do not send anonymous messages.
g. Disruptions – do not use the network in any way that would disrupt use of the network by others.
h. Pupils will not be allowed access to unsupervised and/or unauthorised chat rooms and should not attempt to gain access to them.
i. Staff or students finding unsuitable websites through the school network should report the web address to the IT Helpdesk.

j. Do not introduce USB drives or memory cards into the network without having them checked for viruses.
k. Do not attempt to visit websites that might be considered inappropriate. (Such sites would include those relating to illegal activity). All sites visited leave evidence in the county network if not on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
l. Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to e-mail.
m. Files held on the school's network will be regularly checked by the IT Technicians.
n. 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.

4. UNACCEPTABLE USE

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

a. 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.
b. Users finding machines logged on under other users username should log off the machine whether they intend to use it or not.
c. 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 County Council have filters in place to block e-mails containing language that is or may be deemed to be offensive.)
d. Accessing or creating, transmitting or publishing any defamatory material.
e. Receiving, sending or publishing material that violates copyright law. This includes through Video Conferencing and Web Broadcasting.
f. Receiving, sending or publishing material that violates Data Protection Act or breaching the security this act requires for personal data.
g. Transmitting unsolicited material to other users (including those on other networks).
h. Unauthorised access to data and resources on the school network system or other systems.
i. 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.
j. Users may not play or store games on the network either online or from executables stored on the network. Users found to have games on the network will have them deleted and will be sanctioned appropriately.
k. Users may only store relevant work on the system, users found to have large numbers of pictures or music will have them deleted and will be sanctioned appropriately.

Additional guidelines

l. Users must comply with the acceptable use policy of any other networks that they access.
m. Users must not download software without approval from the IT Technicians.

5. 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.

6. NETWORK SECURITY

Users are expected to inform The Network Manager immediately if a security problem is identified. Do not demonstrate this problem to other users. Users must login with their own user name 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.

7. PHYSICAL SECURITY

Staff users are expected to ensure that portable ICT equipment such as laptops, tablets, 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.

8. 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, sanctions and, if appropriate, legal referral. This includes the creation or uploading of computer viruses. The use of software from unauthorised sources is prohibited.

9. MEDIA PUBLICATIONS

Named images of pupils (e.g. photographs, videos, web broadcasting, TV presentations, 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

Pupils' work will only be published (e.g. photographs, videos, TV presentations, web pages etc) if parental consent has been given.

10. ST WILFRIDS BRING YOUR OWN DEVICE (BYOD) POLICY

a) Overview

We recognise that as technology develops, so more of our students have access to internet capable devices. This should be seen as a resource to provide quick and easy access to learning resources to enhance learning. We should seek to capitalise on the mobile phones and tablet computers our students have and that they should be used in classrooms to support learning where opportunities arise and a mobile device is more appropriate than a laptop or desktop computer.

b) General Information

Access to the wireless network with any device is filtered in compliance with the best practice guidance and in the absence of a UK policy, the US 'Children's Internet Protection Act' (CIPA). Access from a personal device is limited to Internet use only. Pupils will not have access to the school network from their personal devices. Access to the wireless network is a privilege, not a right and access to the network involves personal responsibility and compliance with all school rules. The use of the network allows IT staff to conduct investigations regarding inappropriate Internet use at any time, by teacher request or for other reasons deemed appropriate by the school.

c) Obtaining access to the network

In order to gain access to the network, staff or pupils will need to use the sign up procedures enabling access via the Meraki MDM. This will display the users device name and in some cases their mobile number. Users are advised to change their device name to their username. Before use of the system users will need to instruct the IT Technicians which mobile device belongs to them on the system. Devices will then be named to the students or staff member school user id. Technicians reserve the right to quarantine devices that have not been recognised. Access to the school Wifi system through any personal device will not be allowed by any other system apart from school laptops.

The network access key will be changed every half-term.

d) Guidelines for Use

i) Use of personal devices during the school day is at the discretion of teachers and staff. Pupils must use devices as directed by their teacher.
ii) The primary purpose of the use of personal devices at school is educational. Using the device for personal reasons e.g. contacting parents, should only take place after permission has been given from a teacher or other member of staff.
iii) The use of a personal device is not to be a distraction in any way to teachers or pupils. Personal devices must not disrupt class in any way.
iv) The use of personal devices falls under St Wilfrid's Acceptable Use Policy.
v) Pupils shall not use personal devices outside of their classroom unless otherwise directed by their teacher e.g. on school visits or activities.
vi) Pupils shall make no attempts to circumvent the school's network security and/or filtering policies. This includes setting up proxies and downloading programs to bypass security.
vii) Pupils shall not distribute pictures or video of pupils or staff without their permission (distribution can be as small as emailing/texting to one other person or as large as posting image or video online).

e) Agreed Use During The School Day
   i) During lessons on authorisation of the teacher

f) Use Not Permitted During The School Day
   i) Before School
   ii) Between classes
   iii) Lunchtimes
   iv) The member of staff has disallowed device use in class
   v) Exams (unless permitted by the teacher)
   vi) Assemblies (unless permitted by the teacher delivering the assembly)
   vii) After school

g) Consequences for Misuse/Disruption (one or more may apply):
   i) Access to the wireless network will be removed.
   ii) Device taken away for the period
   iii) Device taken away and kept in the front office until parent picks it up.
   iv) Student is not allowed to use personal devices at school.
   v) Serious misuse of Internet capable devices is regarded as a serious offence within the School's Behaviour Management Policy and will be dealt with in accordance with this policy.

h) School Liability Statement

Pupils bring their devices to use at St Wilfrid's at their own risk. Pupils are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

i) Classroom Rules
   i) Devices should be on silent unless directed.
   ii) Devices must be used purposefully in class.
   iii) Headphones or ear buds can be used to listen on the device as directed.
   iv) No audio, video recording and/or photo taking unless permission is granted from the teacher.
   v) Devices cannot be used during school tests unless permission from the teacher is granted
   vi) Devices should be fully charged prior to the school day.
   vii) Technical or hardware issues are the students responsibility.
   viii) Devices should never be used to cyber bully, harass or to invade staff or students privacy.
   ix) You are responsible for the security of your device.
   x) Devices should not be used during class changeover between lessons.
   xi) When not in use in class devices should be placed screen down on the table

St Wilfrid's is in no way responsible for:
   a. Personal devices that are broken while at school or during school-sponsored activities
   b. Personal devices that are lost or stolen at school or during school-sponsored activities
   c. Maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

J Chandler
Reviewed: 01.12.2015
Review Date: 15/07/2015