ST EUPHEMIA COLLEGE

K-12

COMMUNICATIONS TECHNOLOGY PROCEDURES

2014

Communications Technology Procedures

Introduction

St Euphemia College's Information and Communication Technology (ICT) resources are provided to support and enhance the School's learning activities. ICT resources encompass infrastructure, equipment, software and facilities including technologies such as computers, smart phones, the Internet, broadcasting technologies and telephony.

All of this equipment is provided to enhance the teaching and learning activities at St Euphemia College and should be used for personal use.

Procedures

Students who use the School's computers, network, internet and online communication services must abide by the conditions of acceptable usage. Therefore students from Years 3 to 12, parents and caregivers must sign the agreement for appropriate use of the School's ICT (Appendix 1) before students have access to ICT resources.

Hardware

St Euphemia College maintains 7 computer labs, 2 libraries with multiple computer access and a Video Conferencing Centre. Computer hardware available to the students include:

- desktop computers
- portable computers, such as Laptops/Notebooks and Windows-based tablets
- iPads.

All computers are connected to the School's local area network (LAN) either by an Ethernet connection or wirelessly. All School devices are maintained by the School's ICT consultant and the School's ICT Coordinator, whose task is to maintain security and provide uninterrupted access to all ICT resources.

Students are not to move, damage or disable any of the School's computers, computing devices or computer network equipment. If a student has been found to intentionally damage or restrict any ICT equipment, that student will be given an invoice covering the cost of repairs. Furthermore, at the discretion of the Principal/Delegated Authority or Faculty Coordinator the student will be excluded from using the School's equipment for a specified period.

Personal Mobile Devices

Although staff are allowed to bring to School their personal mobile devices, they are not allowed to use their devices during lessons.

Students are not allowed to bring their personal mobile devices to School. Staff will confiscate any personal mobile device used by students. Confiscated devices will be securely kept at the Front Office for one week. All confiscated devices will be entered into a registry. Confiscated phones may be returned to students if the phone is necessary for afterschool travel arrangements, but must be return to the School the following day.

The School is not responsible for the loss, damage or theft of any personal mobile device. Furthermore, users who bring any personal device to the School must ensure there is no inappropriate or illegal activity or content on the device.

Network/Internet Access

Staff network and email accounts are created once they are employed by the School. They are given a temporary password to which they must change. Any staff given access to the School's ICT facilities must comply with the Communications Technology Policy.

Enrolled students are given a network account once the student and a parent or caregiver has signed the Student Agreement form (Appendix 1). Any student given access to the School's ICT facilities must comply with the Communications Technology Policy.

The School reserves the right to log and monitor all use of the Schools ICT facilities and services. Logs will be routinely monitored to assist in the detection of breaches. Monitoring the use of the School's facilities may be undertaken with or without prior notice to the user.

If an alleged breach is detected or reported which potentially constitutes illegal activity, misconduct, then the matter will be referred to the Principal or Delegated Authority.

Data Access, Storage and Security

All users (staff and students) have access to a personalised drive on the fileserver. Staff and students are encouraged to keep their files on the fileserver so that:

- they may have access to their files irrespective of which computer they use
- their files will be continually backed up
- their files are secured from unauthorised access by other users.

Staff and students are NOT to share their user accounts or passwords. Any student found sharing network accounts, their login access will be disabled and they will be excluded for a specified period of time from using the School's computer equipment.

Staff and student are not allowed to keep inappropriate or offensive material on their network drive. These include:

- footage of real or simulated violence, criminal activity or accidents from video clips or games
- any inappropriate or illegal images of children or adults
- files that promote hatred towards individuals or groups, on the basis of race, religion, sexual preference or other social/cultural factors
- instruction or promotion of crime, violence or unsafe behaviour, like making and/or using drugs, gaining unauthorised access to computers, fraud or terrorist activities

The School has the right to access and view any files kept on its network. If an alleged breach is detected or reported which potentially constitutes illegal activity, misconduct, then the matter will be referred to the Principal or Delegated Authority.

Software

Only software purchased by the School for educational use will be installed on School computers. Unless specifically authorised by the Principal or Delegated Authority, no other software is allowed to be installed or used.

Using the Internet

The School has the responsibility to ensure that all students and staff access the internet safely and responsibly. Safeguards, such as the incorporation of the Fortegate firewall, have been introduced into the School to help ensure all users remain safe while online.

Inappropriate Use:

The filtering of internet content using a firewall provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. A filtering system cannot, however, provide a 100% guarantee of effective filtering. It is the responsibility of staff and students who accidently visit any inappropriate websites to report them to the ICT coordinator.

If any student is caught visiting an inappropriate website, the matter will be referred to the Principal or Delegated Authority.

Cyberbullying is the use of Information Communications Technology (ICT), to deliberately upset others. It differs from other forms of bullying in a number of ways:

- continual invasion of home / personal space. It can take place at anytime, anywhere
- size of the audience. Electronically circulated messages can reach a very large audience, very quickly. The spread of the messages is very hard to limit or control
- anonymity of the bully. The bully may never be in the same physical space as their victim
- the profile of the bully. Age or size is not important. Bystanders can quickly become accessories to the bullying; for example, by passing on humiliating images
- cyberbullying can be unintentional. It can be the result of not thinking or a lack of awareness of the consequences
- many cyberbullying incidents can themselves act as evidence. This is one of the reasons why it is important to know how to respond.

Bullying is never acceptable. The School has a duty to protect all its members and provide a safe and supportive environment.

When dealing with any incident of cyberbullying it is important to follow the procedures set out in the School's Anti Bullying Policy. However, there are some additional steps to take when responding to cyberbullying:

- Reassure the victim that they have done the right thing and that everything will be done to deal with the problem.
- Make sure the person knows not to retaliate or return any messages.
- Help the person to keep any relevant evidence. Note down any web addresses used, take screen capture shots if possible and try to ensure messages are not deleted.
- Advise the person of some simple steps they can take to prevent it from happening again, for example blocking a contact, changing your own contact details, leaving a chat room, reporting the abuse to the service provider.

Action needs to be taken to contain the incident as quickly as possible. Any online content should be removed. In the case of any illegal content, legal authorities may be contacted.

Copyright Issues

The Internet allows access to information, images, musical recordings, films, videos, software and other intellectual property, but it does not mean these things are therefore freely available to copy or download. Material is accessible on the Internet without the copyright owner's permission. St Euphemia's ICT resources must not be used to copy, download, store or transmit material which infringes copyright. Users of the School's ICT resources are responsible for complying with Copyright law (refer to the School's Copyright Policy).

Saint Euphemia College

Appropriate Use of ICT and Internet Services

Student Name: _____ **Class:** _____

STUDENT AGREEMENT (Years 3-12)

I have read and/or discussed the **St Euphemia College Acceptable Use of ICT and Internet Services Policy** and agree to the following:

1. I will use school computers, the Internet and other equipment only with the permission and supervision of a teacher and always for school related activities. I have the responsibility to maintain computer facilities as they have been set up for me and will always save my work in the appropriate place.
2. I will follow all instructions from teachers when using school computers, the Internet and email.
3. I will make sure that any email that I send or any work that I have published uses appropriate language. I will always have my work checked by a teacher before it is published or printed.
4. I accept responsibility for anything that happens to my personal account. I will not let anybody else know what my password is and I will not log into another person's network or email account. I will tell my teacher if I think someone has used my personal account. I have the responsibility to respect the privacy of other people's passwords.
5. I know that the school can see anything that I send or receive, and report infringements to relevant authorities.
6. I will not disclose mine or others personal or family details in emails or anything that is to go online.
7. If I use material in my work that I have found on the Internet, I will acknowledge where it comes from and will always abide by copyright laws. I will ask my teacher's permission before downloading or saving anything from the Internet.
8. If I see any information on the computer that I think is inappropriate or makes me feel uncomfortable I will turn the computer screen off and tell my teacher immediately. I will not respond to any emails that make me feel uncomfortable and will tell my teacher immediately if this happens.
9. I will not become involved in any offensive, bullying or illegal behaviours while using the Internet.
10. I will not damage or disable the computers, computer systems or computer networks of the school or any other organisation.
11. I will only bring information from home on external storage devices (USB device) and use it on school computers with the teacher's permission and supervision.
12. I understand that failure to observe these rules will restrict my access to school computers and Internet facilities and that other disciplinary action may be taken.

Student Name (print): _____

Signature: _____

Date: _____

Parent/Caregiver signature: _____