ICT Acceptable Use
Information and Communication Technology (ICT) Policy

March 2020

RATIONALE

Information and Communication Technology (ICT) encompasses all electronic devices and systems which are used to manipulate or communicate data. It provides schools with the opportunity to promote educational excellence by facilitating communication, innovation and sharing of resources. ICT provides significant educational value but can pose a risk of exposure to inappropriate and offensive material as well as personal safety. In accordance with the teachings of the Catholic Church, the practice of communication must be totally honest and reflect the highest stand of accountability and sensitive to our personal rights and relationships.

PRINCIPLES:

1. The policy concerning student use of ICT shall reflect the teachings and educational goals of the Catholic School. Access to ICT shall be balanced with all elements of the school curriculum.

2. The St Luke's College ICT is provided for educational purposes only. The school encourages students to access ICT on a regular basis to enhance the learning process. Used well, it can have a significantly positive effect on student achievement in all subject areas because it has the potential to: improve student attitudes toward learning and self-concept and make learning more student centred, encourage co-operative learning, improve communication skills, improve participation of students in the learning process and further stimulate student-teacher interaction.

3. Students using the school's ICT must not break State or Federal laws (a summary of these laws is an attachment to this Policy and forms part of this Policy). All rules associated with the use of ICT are founded on these laws and Catholic Church teaching.

4. The school has the right to check all written, graphic, audio, visual and other materials created, produced, communicated, stored or accessed on school ICT by students, including emails and devices.

5. Students shall be made aware that access to ICT and the Internet can expose them to inappropriate material or potential harm.

6. Students shall take personal responsibility when using the school's ICT services by protecting their personal information and data, maintaining the required level of security, respecting the privacy of others, respecting the legal boundaries of licensing and copyright, using language appropriate to the school's expectations and taking good care of all ICT equipment.

Terms and Conditions for uses of Computers, Electronic Devices and Internet Use
St Luke's College is committed to ensuring all students are aware of standards for the use of ICT within the College environment. Consequently, unacceptable use will not be tolerated under any circumstances and disciplinary action will be taken against any student who breaches College policy.

This Acceptable Use Policy may be updated at any point in time. In addition, tools and systems used by the College may be updated, resulting in a change to the Acceptable Use Policy and/or associated conditions for connecting to the network. Please make sure you are referencing the latest Acceptable Use Policy, available on our College website.

1. Privileges
The use of the school's Internet is a privilege, not a right, and inappropriate use will result in temporary or permanent cancellation of this privilege. This includes the freezing of all internet access for the duration of the penalty. Where a serious offence has occurred, this may also include removal of the device for the duration of the penalty.

2. Personal Responsibility
Mandated devices must be present during every class. Devices should be fully charged, and all relevant apps should be downloaded and correctly installed. It is recommended that devices should be purchased according to the recommendations of the 'Bring your Own Device' specification sheet to ensure sufficient functioning for use in the classroom.

Students need to take responsibility for reporting any misuse of computers, electronic devices, software or the College network. The ICT Policy is available on the College website. It is the student's responsibility to be aware of its contents.

3. Unacceptable Use of Computing/Wi-Fi Facilities
Examples include, but are not limited to:
1. Accessing networks without school authorisation
2. Transmitting or deliberately accessing and/or receiving material that may be considered inappropriate, which includes threatening, sexually explicit, or harassing materials, offensive or discriminatory materials, or material that may be harmful either physically or emotionally, which includes bullying or harassment of fellow students or others outside the school
3. Communicating information concerning any password, identifying code or other confidential information or violating the security of the system in any way
4. Interfering with or disrupting network users, services or equipment
5. Plagiarising and/or breaching copyright laws, including software copyright and reengineering of software
6. Conducting private business matters or use the system for any personal gain
7. Downloading and/or installing software programmes on school owned computers and iPads, including videos, music and games without the permission of the College
8. Using video, audio or camera applications on their devices unless given permission by the teacher
9. Posting video, picture or audio files taken in school and during school hours to online networks unless expressly permitted by the teacher

4. Security
Students must keep their password confidential. Sharing of passwords could lead to misuse of resources by other students. To change your current password – please see the ICT Support team.

5. Vandalism
Vandalism refers to any malicious attempt to harm or destroy machinery or data that is connected to the system. This includes uploading and creation of viruses. Vandalism will result in disciplinary action. Where it can be proven that a student has intentionally damaged another device, they will be deemed responsible for the repair or replacement of that device. Disciplinary action in these instances may include, but is not limited to, internal suspension and/or removal of ICT privileges.

6. Guidelines for the use of Ubiquitous Mobile Electronic Devices
Ubiquitous mobile electronic devices include devices such as mobile phones, iPads, Androids, iPods, smartwatches, personal computers, video and digital cameras and graphics calculators.

1. Students who bring valuables to school (including money, debit cards) should place them in their locked lockers during the day. It is crucial that students DO NOT provide their locker combinations to ANY other student.
2. If a student needs to use any mobile electronic device or calculator for a class, they should retrieve the device from their locker in the break preceding the class (e.g. before school, at the end of recess or lunchtime). **Note that mobile phones and iPods/music devices are not allowed in the classroom under any circumstances.**
3. When used in a classroom, the electronic device should be accessed when instructed by the teacher, and turned off when the lesson concludes, or when instructed to do so by the teacher.
4. Mobile phones or portable music devices are not to be used during the school day (from 8.25am until 3pm) for any other purpose. No calls or text messages are to be made or taken during school hours. Emergency calls by parents are to be directed to the administration in the front office.
5. When not in use devices should be closed or placed flat on the desk
6. The College will not be responsible for the loss, misuse or damage of mobile electronic devices, or any other valuables.
7. **Mobile phones will be confiscated if the guidelines listed are not followed. A mobile phone may be collected once written consent has been received from a parent/guardian.**
8. **Mandated devices are for educational purposes only. Teachers reserve the right to delete any apps that are deemed inappropriate and may carry out random checks to ensure that policy guidelines are being followed.**
9. **If a student is in breach of any of the guidelines and the device in question does not belong to them, then both the student in question and the owner of the device will be subject to the full penalty as outlined in the ICT policy**

7. Printing
St Luke's College recognises that printing of hard copy by students is sometimes necessary. However, students should aim to keep the volume, and hence the cost, of printing to a minimum. This can be achieved by print previewing, spell checking before printing, editing on screen or transferring by other electronic means rather than continuous printouts and printing double-sided where possible. Students must not load paper into printers without permission. Printing should be directly related to schoolwork.

8. Internet Downloads
St Luke's College is charged for downloads by our Internet Service provider and cannot allow unlimited downloading by students. Students should behave as responsible Internet users and aim to keep the volume, and hence the cost, of downloads to an acceptable level.
Transferring any file from a computer on the Internet to your computer constitutes a download. Student downloads should be directly related to schoolwork.
Because the Internet is an unsupervised environment, the school has a responsibility to ensure that, as far as possible, material obtained from the Internet is not offensive or inappropriate. To this end, filtering software has been implemented. In the end, however, it is the responsibility of individual students to ensure their behaviour does not contravene College rules or rules imposed by parents/carers.

9. School Communications and Online Chat Systems
Realtime Chat Programs are not to be used by students unless the classroom teacher has given approval. *Examples include Skype, iChat, Facebook, MSN Messenger, Tumblr, Twitter, Myspace, Snapchat.*

10. Device Management

Given the large number of devices on the College network, the ICT Support Team employ digital tools to assist with the monitoring, asset management and software management for all devices connected to the College network. As such, it is a condition that any device connected to the College network has the appropriate monitoring tool operating. These tools provide the ICT Team with statistical information surrounding the use of software and hardware information along with the ability to distribute software, updates and security patches to all network computers. It also provides the ICT Team with the ability to remotely support clients when connected to the College network.

1. Personal devices, once connected to the network, should only be used in classes whereby teachers have expressly permitted their use.
2. Students:
    a. *are required to maintain and clean their device. It is suggested that, as a minimum standard for backing update procedures, **all devices** on the College network be backed up **at least twice a week**. The ICT Support staff helps any student who has an issue with this process.*
    b. *are required to report any damage immediately to the ICT Support Team.*
    c. *are required to inform the teacher or others when using the camera and audio recording functions and are reminded that it is an offence to publish photographs to any online network.*
    d. *are required to actively check their email for communications from the College.*
    e. *may not loan their device to another student or leave it in such a place that it is likely to be easily stolen.*

11. ROLE OF THE FAMILY

If students choose to ignore these procedures the following process will apply:

1. *Offence I*   *A lunchbreak consequence, parent/guardian contact made through SEQTA*
2. *Offence II*   *A lunchbreak consequence, parent/guardian contact made through SEQTA*
3. *Offence III*   *Internal suspension and an interview with parent/guardian arranged*

The Deputy Principals will oversee this process in consultation with appropriate members of the Pastoral and Learning Teams in the College.

12. COLLECTION NOTICE

Personal information collected from students is regularly disclosed to their parents or carers. On occasions information such as academic and sporting achievements, student activities and other news is published in College newsletters, magazines, local newspapers and on our website. If you do not wish to have our child's name or photograph published in these mediums, then this request needs to be put to the Principal, in writing.

13. MONITORING

All students and parents should be aware that the Catholic Education WA monitors all student emails and redirects student emails which contain obscenities. All students in Catholic schools in Western Australia are subjected to this filtering. The filtering system automatically detects inappropriate emails and forwards these to the College network managers instead of the intended recipient. Students will have privileges removed as stated above if this is in breach of the College acceptable use policy.

Important statutes which are applicable to students' use of school ICT include:

Copyright Act 1968 (Cth)
Students may copy or otherwise deal with copyright material for the purpose of study or education. However, generally only the author of original material has the right to reproduce, copy, publish, perform, communicate to the publican and make an adaptation of the copyright material.

Equal Opportunity Act 1984 (WA)
This Act precludes:
- Discrimination against persons on grounds of sex, marital status or pregnancy, family responsibility or family status, sexual orientation, race, religious or political conviction, impairment or age in education.
- Sexual harassment and racial harassment in the workplace and in educational institutions

This Act promotes
- Community recognition and acceptance of the equality of all persons regardless of their race, sexual orientation, religious or political convictions, impairments or ages.

Censorship Act 1996 (WA)
Students must not use a computer service to transmit, obtain or request an article knowing that it contains objectionable and restricted material. It is an offence to possess or copy indecent or obscene articles or child pornography. Students should be aware for their own protection that people who deal with such material commit an offence.

Criminal Code (WA)
Students should be aware that it is illegal to show offensive material to children under 16, and that if someone does show them offensive material that person is committing an offence. Racist harassment and incitement to racial hatred are also criminal offences.

Cybercrime Act 2011 (Cth)
Unauthorised access to or modification of data held in a computer and unauthorised impairment of electronic communication e.g. 'hacking' or inflecting computer systems with a virus, are illegal.

Privacy Act 1988 (Cth)
Students should respect that the personal information of others is private. This Act covers the collection, use and disclosure, quality and security of personal information.