URSULA FRAYNE CATHOLIC COLLEGE

INFORMATION & COMMUNICATION TECHNOLOGY POLICY
& USAGE AGREEMENT (STUDENTS YEARS 7-12)
Student Owned Devices

Rationale

Information and Communication Technology (ICT) is utilised in schools for learning, teaching and administration. The availability of such resources provides the opportunity for schools to help students develop their full potential. ICT provides significant educational value but can pose risks regarding safety, personal reputation and corporate reputation.

In accordance with the teachings of the Catholic Church, the practice of communication must reflect the highest standard of accountability and sensitivity to human rights and relationships.

Definitions

'Information and Communication Technology (ICT)' means all hardware, software, systems and technology including the internet, email, telecommunications devices *(e.g. mobile phones)* and social media *(e.g. facebook).*

'Device' - means the ICT appliance designated by the College and specified on the College year level Booklist.

Principles

1. The Ursula Frayne Catholic College ICT program is provided for educational purposes only.

2. Using the Ursula Frayne Catholic College ICT is a privilege. This privilege can be removed if school rules are broken. Students using the school's ICT must not break State or Federal laws.

3. To maintain a sense of equity and consistency, students must purchase the device specified by the College.

4. While the device is owned by the student, the device is to be used solely for educational purposes directed by the College.

5. As a matter of duty of care, the College has the right to check all written, graphic, audio and other materials created, produced, communicated, stored or accessed on school ICT by students, including through social media.

6. Students shall be made aware that access to ICT and, in particular, the Internet and social media, can expose them to inappropriate material or potential harm.

7. 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.

Procedures

1. **Security of the device**
   Students are responsible for the security of their device at all times. Students are expected to keep their device in their locker or have it with them in times of use. During school time when the device is not being used it must be stored in the student's locker and the locker must be kept locked using an official College lock.

   Students must ensure that all passwords and data are stored securely. In addition, students are advised to regularly backup their work and information. The College takes no responsibility for the loss of data.

2. **When should a device be brought to Class?**
   Unless specifically advised otherwise by their teacher, students should bring their device every day to all classes. Many classes will require the formal use of devices, while others will provide informal opportunities to use technology to complete tasks efficiently. It is imperative that the device be available for use at the teacher's discretion.

3. **Leaving the device at home**
   Students are encouraged to take their device home each day to assist in completing homework and study. However, students who do not bring their device to school for any reason may be unable to complete classroom activities appropriately and will be expected to make up the lost time. Students who continually fail to bring their device to class may be subject to disciplinary action. The College will not provide loan devices.

4. **Charging batteries**
   Students should arrive at school with their batteries fully charged. This should be a part of a normal homework routine and students arriving at school without their device charged and ready, or without their power cord, may be unable to complete classroom activities appropriately and will be expected to make up the lost time. Students who continually fail to charge their batteries may be subject to disciplinary action.

   Provision may be available in class for connection of the device to the mains power in cases where extensive use of the device during the day has caused the batteries to become discharged. With appropriate power conservation settings and use of sleep features, a fully charged battery should last most of the day. Students should work to lengthen battery availability by placing it in sleep mode whenever not in use during the day.

5. **Role of Parents**
   Parents are asked to supervise the security of the device while at home, or in the car, and to assist students with making sure that devices are stowed securely in the school backpack while in transit to and from school. Parents are requested to take particular care over the supervision and access of other members of the family to the device.

   While it is reasonable to expect that other members of the family may benefit educationally from the device from time to time, this should not occur in a way that restricts the student from having full access when needed both at school and at home.

   Parents are asked to assist in making sure that the fully charged device comes to school with the student every normal school day. Students are discouraged from regularly leaving the device in their locker overnight.

6. **Virus Protection**

Students have the responsibility to minimise the risk of receiving computer viruses. Viruses have the potential to severely damage and disrupt normal operations of the device and networks. As students have the opportunity to connect to the internet from home, they should take all steps to protect the device from virus attacks.

Viruses can enter devices through:
- Removable media such as USB memory sticks;
- Emails and the internet (including web browsing, FTP programs and chat rooms); and
- File download/Network file shares, such as servers and shared folders.

Virus Protection Tips:
- Protect your device from virus attacks by scanning your device for viruses at least weekly.
- Consider carrying out a virus scan of your device after you have accessed the internet or personal email or opened a file from a removable media source. You should carry out the scan before returning to the school and connecting to the College network.
- Do not use your device to access any email account apart from your College webmail account.
- Do not open any files attached to suspicious or unknown emails.
- Exercise caution when downloading files from the internet.
- Delete chain and junk emails. Do not forward or reply to any of these.
- Never reply to spam. Spam email messages can contain viruses that notify a third party of the legitimacy of an email address and then add the recipients to the spammer's database.

7. **Occupational Health and Safety**

Instruction on the use of ICT devices in a good ergonomic environment will be part of the teaching and learning process. This will focus on good posture with attention to the position of the chair, desk and ICT device, as well as demonstration of stretches and other exercises. Additionally, students will be advised to avoid looking at the screen for extended periods of time.

8. **Insurance, Warranty and Repairs**

Insurance of the device is the responsibility of students and parents.

Since the device is purchased by the student/parents, any warranty or repairs are a negotiated agreement between the parents and seller. Repair and replacement costs for ancillary items such as cables and battery charges are the responsibility of parents.

9. **Technical Support**

The College ICT Department will provide low level troubleshooting to fix minor software issues and faults. Students can access this service by visiting the ICT Help Desk before school, at recess or lunch breaks, or after school.

10. **Acceptable and Unacceptable Use**

Ursula Frayne Catholic College is committed to ensuring that all students are aware of standards for use of ICT within the school environment. Consequently, unacceptable use will not be tolerated under any circumstances and disciplinary action will be taken against any student who breaches this policy.

Matters constituting acceptable and unacceptable use of ICT are listed below:

10.1 Acceptable use:

- researching information relating to assignments; *
- gathering specific information about assigned subjects/topics/tasks; *

❑   communicating with a teacher or friend for assistance with school related work; and

❑   other teacher directed activities.

  * *Students shall exercise caution as to the quality and accuracy of the information they are accessing or transmitting.*

  10.2   Unacceptable use:

  10.2.1   **Unacceptable use includes but is not limited to:**

❑   accessing networks without school authorisation;

❑   utilising anonymiser sites, or equivalents, to by-pass proxy servers or normal filtering systems on the College networks.

❑   transmitting or deliberately accessing and/or receiving material that may be considered inappropriate, which includes threatening, sexually explicit, or harassing materials, 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;

❑   communicating any information concerning any password, identifying code or other confidential information or violating the system in any way;

❑   interfering with or disrupting network users, services or equipment. Disruptions include but are not limited to, distribution of unsolicited advertising, propagation of viruses in any form, and using the network to make unauthorised entry to any other machine accessible via the school's network (ie 'hacking');

❑   plagiarising and/or breaching copyright laws, including software copyright and re-engineering of software;

❑   conducting private business matters or using the system for any personal gain; and

❑   downloading and/or installing software programs (eg .exe files), videos, music, picture galleries, greeting cards, screen savers and games, etc without the permission of the school.

  10.2.2   **It is unlawful to use ICT which:**

❑   defame someone or an organisation;

❑   infringe copyright laws, ie reproduce or adapt copyrighted material by downloading and further disseminating the material;

❑   contain statements which could constitute sexual discrimination or sexual harassment;

❑   display sexually offensive or explicit material;

❑   contain offensive or insulting statements based on the race, colour or nationality of a person; and,

❑   undertake activities which breach State and Federal legislation.

11.   Unacceptable and/or unlawful use of ICT constitutes a breach of school rules and may warrant disciplinary action.

If students are unsure about any issue in the College ICT policy it is their responsibility to seek clarification before they act.

Legal action may be taken if illegal acts are committed.

I understand that failure to observe the terms of this agreement is a breach of my Enrolment Agreement and may result in my access to the use of College ICT being restricted and, where appropriate, other sanctions being invoked.

I understand the above conditions and agree to abide by them when using ICT at Ursula Frayne Catholic College.

Student's Name: _____ Form: _____

Student's Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____