St Francis of Assisi College

ICT POLICY

Rationale

This policy provides detailed principles and procedures to ensure all students and staff are aware of their responsibilities and obligations when using ICT equipment and resources at the College.

At St Francis of Assisi College, we support the rights of all members of the school community to be provided with, and engage in a safe, inclusive, and supportive learning environment. This extends to the use of digital tools and online communities and is underpinned by our expectation of safe and responsible behaviour of all members of the school community. St Francis of Assisi College uses the Internet and digital technologies as a learning tool to improve student learning outcomes, by increasing access to worldwide information and platforms to foster the skills required to be successful in a world where technology is ubiquitous.

Our school embraces the benefits of technology and is committed to reducing students' exposure to cyber risks. Within this context, the objective of this policy is to ensure smart, safe, and responsible use of digital technologies and Internet within our school community.

Access to all ICT facilities and resources are a privilege and not a right. Inappropriate use will involve corrective action and could result in confiscation of equipment, exclusion from accessing ICT resources and equipment or an external police investigation.

This policy should be read in conjunction with St Francis of Assisi College ICT User Agreement, Mobile Communication Device Policy, Anti-Harassment Policy, DPR Policy and Laptop Code of Conduct.

Introduction

St Francis of Assisi College provides an extensive range of information and communication technology equipment, resources and services to students and staff.

The College Board and Leadership Team expect responsible use of Information and Communication Technologies (ICTs) by all students and staff both on and off campus. This includes the use of all computing hardware, software, email, Internet, intranet, social networking sites and College information systems.

Please note the College cannot accept responsibility for the loss, damage or theft of any personal property belonging to staff or students.

Definitions

- **Bullying** refers to any intentional and repeated behaviour which causes physical, emotional or social harm to a person who has, or is perceived to have, less power than the person who bullies (Australian Education Authorities 2019; Kids Helpline 2019; Australian Human Rights Commission 2012).

- **Cyberbullying** is bullying with the use of digital technology. For example; using the Internet, gaming platforms or social media to hurt, harass or embarrass someone.

- **Cyber Safety** is the act of taking precautions to protect and maintain anonymity of your own and/or another person's security and wellbeing when connecting and interacting with people in an online environment.

- **Digital Citizenship** is a set of skills and behaviours required to be a successful learner, confident individual and effective contributor in today's digital age.

- **Digital Literacy** is the knowledge, skills and behaviours required to use a broad range of digital devices to critically navigate, evaluate and create information and develop new social and economic opportunities for oneself and others in the community.

- **Digital Technologies** are electronic devices, systems and resources that generate, store or process data. In this document it includes, but is not limited to, computer workstations, notebooks, cameras, smart phones, tablets, video and audio players/recorders, social media and networking sites and cloud solutions.

- **eSmart** means knowing how to guard against security and privacy risks online, download content in a legal and ethical way, research and reference information, as well as manage reputation and relationships in cyberspace (The Alannah and Madeline Foundation).

- **Social Media** is computer-mediated services that are used as a means of supporting interactions among people and organisations in which they create, share and exchange information and ideas (for example: Twitter, Facebook, Instagram, Tumblr, Snapchat).

1. **Purpose**

   This policy aims to:

1.1 Provide a safe, secure and caring learning environment.
1.2 Develop safe practices for the use of the Internet and digital technologies for learning.
1.3 Establish transparent expectations for students, teachers and the community when using the Internet and Digital Technologies.
1.4 Assist students and members of the school community to differentiate between bullying and inappropriate social interactions.
1.5 Foster social responsibility in all students so that they report inappropriate behaviour towards others rather than act as bystanders.
1.6 Recognise that explicitly teaching students about safe and responsible eSmart behaviour is essential in the lives of students and is best taught in partnership between home and school.

2. Broad Guidelines

2.1 St Francis of Assisi College's User Agreement is shared with students and parents.

2.2 All students must have submitted an EdSmart form acknowledging the User Agreement.

2.3 A copy of all school ICT policies and user agreements are displayed on the school website.

2.4 Breaches of User Agreements are recorded and are dealt with accordingly.

2.5 The College community will be updated on a regular basis through newsletters, social media, special events and the College website.

2.6 Safe and responsible use of technology in line with St Francis of Assisi College ethos, vision and mission, will be taught in all year levels.

3. Implementation

3.1 Members of Staff at St Francis of Assisi College have the responsibility to ensure that:

3.1.1 They are familiar with eSmart approaches and understand the philosophies of the eSmart program, necessary for teaching digital literacy.

3.1.2 They are aware of cyberbullying and able to identify and look for signs of occurrence amongst students.

3.1.3 Students are aware that any form of cyberbullying is prohibited at St Francis of Assisi College.

3.1.4 Students are aware of the consequences of cyberbullying.

3.1.5 All cases of cyberbullying are reported to Leader of Wellbeing and Home Group teacher and responded to promptly.

3.1.6 There is effective supervision of digital technology usage in Learning Spaces and the school to monitor and deter cyberbullying.

3.1.7 They understand copyright laws and understand it is illegal to copy any software, graphics, text, games or digital media that contravenes copyright laws.

3.1.8 All files and materials created using St Francis of Assisi College equipment and resources are deemed to be the property of the College. This includes the access of College information and resources from outside the school.

3.2 Students at St Francis of Assisi College have the responsibility to ensure that:

3.2.1 The St Francis of Assisi College ethos, vision and mission are demonstrated when using digital technologies.

3.2.2 Only approved digital technologies are used in accordance with the User Agreement and in line with the school curriculum program.

3.2.3 They do not breach the privacy of students, staff and members of the school community through any unauthorised publishing of photography, video, or defamatory comments on social media or networking sites and applications.

3.2.4 All incidents of cyberbullying are reported to a member of staff.

3.2.5 They take steps to protect their own (and others) privacy and personally identifiable information.

3.2.6 Copying files, passwords or work belonging to another person may be deemed plagiarism and/or theft.

3.3 Parents at St Francis of Assisi College have the responsibility to ensure that they:

3.3.1   Are familiar with the College's User Agreement so they can support their child to adhere to the expectations set out in the document.

3.3.2   Report any incident of cyberbullying or unsafe cyber behaviour that they become aware of, to the College as soon as possible.

3.3.3   Respect the privacy of students, staff and members of the College community through only authorised uploading, recording or filming.

4. Incidents and Complaints

4.1   Any form of bullying, whether physical, verbal or cyber, is unacceptable.

4.2   All incidents of cyberbullying must be reported to a staff member.

4.3   Incidents will be investigated and recorded in a register maintained at the school.

4.4   Students have a secure way to report cyberbullying or other incidents involving technology that cause them concern.

4.5   All teachers have a responsibility to respond to, investigate, follow up and monitor incidents of cyberbullying.

4.6   Any parent who believes that their child is being cyberbullied should contact the school. In the first instance, contact will be with the classroom teacher or home group and then the Leader of Wellbeing, APRIM or Principal.

4.7   Parents will be notified if students are involved in any incidents of cyberbullying and appropriate and proportional consequences will be followed.

ICT POLICY approved by:			
SIGNED (Principal or Delegate)		Date:	
SIGNED (Board Chair)		Date:	
SIGNED (Responsible Leadership Member)		Date:	
POLICY TO BE REVIEWED BY (person/role):		Review Date:	