



St Francis Xavier College Digital Technology Use and Responsibility Procedure

Introduction

St Francis Xavier College recognises that access to technology in school gives students and staff greater opportunities to learn, engage, communicate and develop skills that will prepare them for work, life, and citizenship. The College is committed to the development of individual technology and communication skills.

All access to technologies provided by St Francis Xavier College are intended for education purposes. This policy outlines the guidelines and behaviours that users are expected to follow when using school technologies or when using personally- owned devices.

Rationale

The purpose of this policy is to set standards of behaviours for the use of digital technologies and social media that are consistent with the broader values and expectations of the St Francis Xavier College Community. Furthermore, this policy ensures the appropriate, effective and equitable use of the college network.

Definition

This policy refers to all use of computers including, internet access, desktop computers, mobile computers or devices, videoconferencing capabilities and online collaboration capabilities. Social media is any form of web-based publication, forum or presence that allows interactive communication, including, but is not limited to, social media, blogs, forums, discussion boards, chat rooms, and wikis.

Scope

As digital technologies emerge, St Francis Xavier College reviews their suitability for application to the learning goals of the College and will attempt to provide access accordingly. The policies outlined in this document are intended to cover all available technologies, not only those specifically listed.

Rights & Responsibilities

Individual behaviour on the school computer network is expected to be in accordance with the College's Discipline Policy relating to general school behaviour. While making every reasonable effort to ensure students' safety and security online, the College is aware that the nature of this resource can provide opportunities for inappropriate use. Intentional, unacceptable, or irresponsible use of the internet or computer facilities will result in disciplinary action that may result in the suspension or revoking of privileges. Threats to network security or breach of data should be immediately reported to the Digital Technology Team.

Examples of unacceptable computer network use are:

- Sharing of individual passwords,
- Using the account of another student, teacher or staff member,
- Gaining unauthorised access to files, or vandalising the data of another user,



- Accessing material that is obscene, violent or offensive,
- Harassing, threatening or intentionally degrading others by means of the internet including all forms of social networking, e.g. Facebook, Twitter, Instagram, SnapChat, TikTok etc.,
- Bypassing data filtering defences, or similar activity contrary to intended use of the network,
- Intentionally damaging or disrupting equipment or software,
- Using the network or equipment for illegal activity or distributing illegal digital material, including chain letters,
- Using the College's computing resources for commercial or financial gain or fraud,
- Violating web publishing content guidelines,
- Uploading, or otherwise making available, files that contain images, software or other material protected by copyright and intellectual property laws unless you own or control the rights, or have appropriate consent from the owner.

Content Guidelines – Publishing Online

Staff and students collaborating online or producing material for publication on the internet within public or protected spaces such as social media, websites, blogs, wikis, bulletin boards, chat, video and audio sharing services, and similar, must:

- Be aware of potential public audience for all online publication,
- Refrain from publishing personal information about self or family that may impact on personal safety, e.g. photographs, surname, address, telephone numbers,
- Never post information, images or identification of others without their permission,
- Never post on behalf of the college community anonymously without the knowledge of the Marketing Manager,
- Refrain from use of profane, bullying or defaming language that will bring the college into disrepute.
- Refrain from use of college intellectual property or branding (logos) without authority of the Principal.

Content Guidelines – Use of social media content within the College Curriculum

(Please also refer to the DOSCEL [social media policy](#))

Social media channels can at time present information in a quick and easy manner. The College understands the importance of utilising a range of resources that can support student learning.

As part of this approach, it would be suitable to provide guidance on the best practice when accessing information from social media channels. Some points include:

- The use of social media is not endorsed or promoted by the College for young people.
- When doing research for learning tasks, it is best to go to the source (ie: the website of the organisation).



- It is reasonable to outline that if students do use social media, there are groups you can follow for more accurate information.
- In these cases we would not explicitly direct to any particular social media platform/s

Email/Chat Guidelines

Email/Teams Chat is an official method of communication within the college. Members of the College Community are expected to check their email/chat regularly.

Guidelines:

- M365 accounts are expected to be used for school related activity. Sending of chain mail, spam and similar material is unacceptable,
- Email/Chat may not be accessed during class time without teacher consent,
- Examples of inappropriate use of email/chat are as listed above and include sexting and threatening emails.
- Official email signature to be displayed on communications (staff).

Consequences

Intentional inappropriate use of the internet or college computer facilities will result in disciplinary action that may result in the suspension or revoking of access privileges. Serious misconduct may result in more serious action by the College.

The Principal has ultimate authority over the use of all college network resources and associated applications. The Principal (or nominated representative) may review patron files and communications as necessary to maintain system integrity and ensure responsible use. Consequently, no guarantee of complete privacy is made by this policy.

Students are not to intentionally use the computer for inappropriate, harmful or any illegal purpose such as:

- cyber-bullying;
- harassment;
- accessing pornography;
- criminal activity (cyber-stalking, threats);
- uploading in any context: images of College logo, teachers, uniforms or buildings on to the internet (without written consent from the College);
- defaming the College or staff; or
- bringing the College into disrepute.



St Francis Xavier College

Berwick, Officer and Beaconsfield

Review

A review of the Digital Technology Use and Responsibility Policy will be conducted should the College Executive deem it necessary or alterations to the relevant legislation occur.

St Francis Xavier College Digital Technology Use and Responsibility Policy
(Updated 2022)