St Francis de Sales
COLLEGE

ICT ACCEPTABLE USE POLICY

APPROVAL OF:	ICT Acceptable Use Policy
Acting Principal	Paul Wadsworth
College Board Chair	Nick Crowe
Date	November 2023
Next Review	November 2025
Responsible Officer	Principal through the Deputy Principal - Learning

CONTENTS

VISION STATEMENT

St Francis de Sales College aspires to be a leader in education serving the Adelaide Hills community. Grounded in our catholic values and in partnership with families, all community members are known and loved as an individual in the image of God.

Providing a contemporary and inclusive education, relationship and engagement empowers students to be self-motivated, creative and courageous learners.

Our students' growth mindset inspires them to achieve their personal best in all aspects of their school life and develops confident graduates eager to impact their local and global community.

OUR MISSION

"Be who you are and be that well."

RATIONALE

The Melbourne Declaration on the Educational Goals for Young Australians (MCEETYA 2008) recognises that we live in a digital age that is rapidly changing. It states that 'Young people need to be highly skilled in the way they share, use, develop and communicate with ICT. To participate in a knowledge-based economy and be empowered within a technologically sophisticated society now and into the future, students need the knowledge, skills and confidence to make ICT work for them at school, at home, and in their communities. The Alice Springs (Mparntwe) Education Declaration (2019) provides further guidance on the importance of ICT in schools, indicating that 'in an information and technology rich society we must ensure that educators are supported to continually develop their own skills, in order to teach young Australians, the essential skills and core knowledge needed for a modern society and economy'. It continues, saying schools are striving to produce students who 'are successful lifelong learners who are productive and informed users of technology as a vehicle for information gathering and sharing, and are able to adapt to emerging technologies into the future.'

At St Francis de Sales College (SFdS), we understand the powerful contribution that digital technologies (including the Internet and other forms of information and communications technology) can make to the development of contemporary and quality teaching and excellent learning outcomes. We celebrate the capacity of new technologies and are committed to providing staff and students with quality ICT information, infrastructure and resources to enhance learning environments throughout and beyond the College.

At St Francis de Sales College, we use ICT information, infrastructure and resources in harmony with the Catholic ethos of the College and in keeping with the College's Heart Values. This Policy establishes the principles regarding safe, responsible and lawful use of ICT information, infrastructure and resources within and related to our College.

Whilst acknowledging the important role of ICT tools and services within the College, it is essential we protect the integrity, confidentiality and security of all school data, and that all employees and students act in accordance with our College Policies to ensure we minimise the risk of potential threats.

Access to the College ICT networks, infrastructure and data is a privilege and all employees, students and workplace participants seeking access to the College network must consent to and sign this ICT Acceptable Use Policy prior to connecting to the College network or utilising College resources.

SCOPE

The ICT Acceptable Use Policy outlines the standards, guidelines and ethical use expectations and obligations of all ICT and Social Media users at St Francis de Sales College.

This Policy applies to:

- All staff, students and workplace participants of St Francis de Sales College, including volunteers and contractors, who are authorised by the Principal, or delegate, to have access to the College's ICT resources.
- The use of all ICT resources owned or operated by the College at any time, whether during or outside of school hours, and includes the use of remote access facilities
- The use of any personal ICT devices and/or Social Media (including outside of normal working hours and including remote use) where such use:
    - Is likely to cause serious damage to the relationship between SFdS and the student or employee or workplace participant, or
    - Is likely to damage the interests of SFdS, or
    - Is incompatible with the student's or employee's or workplace participant's duty to SFdS
- All software and hardware, whether owned and supplied by the College or not, including that which staff and students have acquired for personal use but are not licensed or formally approved by the College
- Any use of ICT or Social Media that contravenes any other St Francis de Sales or CESA policy, standards or guidelines

This Policy is to be read in accordance with associated policies of Catholic Education SA (CESA), South Australian Commission for Catholic Schools (SACCS) and the College, with specific reference to those in Appendix 1.

POLICY PRINCIPLES

1. Responsibilities for implementation, monitoring and continual improvement

1.1 The use of SFdS ICT Facilities (including the use of Personal ICT Devices to access material on the College's network and services) should be consistent with the Catholic ethos of the College. Any reference to Catholicism, Catholic Church, Catholic Schools, the Pope, the Bishop and other clergy, the SFdS College must be consistent with obligations to uphold the Catholic ethos of our College.

1.2 In using SFdS facilities or personal ICT devices that access material on the College's network and services, all users must:

- Act ethically and responsibly in all dealings with others
- Observe obligations regarding confidentiality and privacy of personal information, in accordance with the College's Privacy Policy
- Maintain a secure password and ensure they do not provide the password to anyone else
- Not attempt to gain unauthorized access to other people's account or user information, or otherwise attempt to defeat any security controls
- Not use another person's email account or other means of communication to send any communication in that other person's name (unless authorised by that person)
- Not take photos or video of members of the College community without their consent, excluding security cameras operating within the College and where appropriate signage indicates their use
- Ensure they do not permit or facilitate unauthorized use of the SFdS ICT facilities by anyone
- Promptly report any evidence or reasonable suspicion of unauthorized access/use to SFdS leadership
- Promptly report any accidental access to inappropriate material
- Ensure intellectual property rights and copyright are not violated

1.3 The College's ICT infrastructure and resources are educational and business facilities, to be used primarily for educational purposes.

1.4 All documents and data created and stored on the network will be treated as education-related and are the property of the College. Accordingly, users should not expect that any information or document transmitted or stored on the network is private.

1.5 Personal devices that access material on the College's network and services may be used by staff and students under the following conditions:

- The device is being used to undertake College business or meet educational requirements in line with ICT acceptable use guidelines, as if such equipment were supplied by the College
- The device is protected with a secure password or PIN.
- Passwords must be at least 10 characters in length, a combination of upper/lower case letters and special characters. Passwords must be changed at least every 6 months
- Images captured for learning and assessment are removed from the device at the end of the activity
- The device may be monitored by the College
- If necessary, the device must be provided to College authorities for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred

1.6 Incidental personal use of devices is permitted if the use:

- Is minimal
- Conforms to SACCS, CESA and College policies and processes
- Does not hinder a staff member's performance of their duty and productivity
- Does not interfere with students learning and productivity
- Does not involve the storing or downloading of large files (including music or movies) for personal use

1.7 Users must take steps to prevent unauthorised access to ICT resources by maintaining secure passwords and protecting devices from access by other users.

1.8 Usage of the College's ICT resources for social networking is restricted to selected staff members approved by the Principal, and can only be accessed strictly in accordance with this Policy.

2. Unacceptable Use of ICT

2.1 SFdS ICT facilities or Personal ICT devices that access material on the College's network and services must not be used to:

- Send or publish any statement, image or other material that is offensive or threatening, or could constitute harassment, discrimination, vilification, defamation or cyberbullying

- Send, post or publish to any personal social media or platform, or communicate by any carriage service, any photographs or images of any student or any activity in which students are participating, without the written permission of the Principal or other delegated person with appropriate authority
- Knowingly access, download, store, send or publish any material that is pornographic
- Do anything that the user knows, or reasonably suspects could contravene the law, including without limitation downloading material in breach of copyright
- Send or help to send unsolicited, non-College, bulk email (spam)
- Open or download any attachment, or access any link, the student, employee or workplace participant reasonably suspects may contain a virus, malware or other computer contaminant (any such attachment or link should be forwarded to the SFdS ICT personnel for review)
- Obtain unauthorised access to the SFdS or any other network, or to deliberately degrade the performance of the SFdS data network
- Install any unlicensed or non-approved software onto computers or other communication devices supplied by SFdS
- Use SFdS network and services to cheat, collude or plagiarise

2.2 Users must not use College credentials (including email addresses) for private activities such as banking or subscription services.

2.3 Users must not attempt to gain unauthorised access to anyone else's account, device or user information.

2.4 Users must not attempt to defeat any SFdS network security controls, including installation of any VPN or similar software on College devices. If installed on private devices, VPN software and connection must be inactive while attending the College and connecting to the College network.

3. Monitoring and Compliance

3.1 The College will implement and monitor systems to ensure College facilities are protected and used in responsible, safe and lawful ways.

3.2 All users accessing or using ICT resources provided by the College accept that use will be monitored, and any evidence of use that contravenes this policy, or is otherwise inappropriate, may lead to disciplinary action.

3.3 The College reserves the right to audit privately owned ICT electronic devices and equipment used on the College site or to access the College resources (on or offsite) to ensure the College ICT Acceptable Use Policy and Personal Responsibility Policy are upheld at all times. This includes personal web browsing, social media access and emails (sent and received) using College ICT resources.

3.4 Connectivity of all staff devices will be centrally manage by the College ICT Department, and configurations will be in accordance with guidelines in place to protect and secure College data, information systems and storage. Configuration of devices will include password protection and encryption, and any othe controls essential to isolating and protecting sensitive information accessed from or stored upon personal devices or the College network.

3.5 Policies applying to BYOD devices will be centrally managed if when installing Office 365 students and/or parents/caregivers select the BYOD device to be managed by the College

3.6 Breaches of Policy principles and guidelines may result in loss of privileges including loss of access to ICT facilities or further disciplinary procedures as deemed appropriate.

3.7 Where a device that contains SFdS data is lost or stolen, SFdS authorities reserve the right to erase all data on the device (including any personal data).

4. Staying safe online

4.1 Personal devices that access material on the SFdS network and services must be protected with a secure password and/or PIN.

4.2 When posting material in a Social Media forum (eg: Facebook page, Twitter, blog, etc…) students, employees and workplace participants should be aware that such activity is considered public, not private.

4.3 Students are to report to an adult if they, or one of their peers, accesses a website or sees something online that makes them feel uncomfortable.

5. Cyberbullying

5.1 Although cyberbullying may occur off site and out of school hours, the College will address these matters if it is deemed they are impacting on the relationships of students within the College.

5.2 Students are to report to an adult if they, or one of their peers, is being bullied online.

5.3 If possible, students/parents are to collect evidence of cyberbullying by photographing or printing the screen and provide this evidence when raising the matter with the College.

5.4 These matters will be addressed in line with the Personal Responsibility Procedures.

6. Responsibilities

6.1 Responsibilities of the College

Additional responsibilities of the College in relation to ICT Acceptable Use are to:

- Implement appropriate measure to enable compliance with this policy, including appropriate monitoring and identification of any breaches
- Ensure all students, parents, employees and workplace participants sign the Acceptable Use Agreement at the beginning of each year, or when they start at the College throughout the year
- Ensure appropriate storage of Acceptable Use Agreements
- Ensure regular professional development sessions are conducted for staff and informal reminders are issued in relation to the College's Acceptable Use Policy and the Acceptable Use Agreement and that new employees and workplace participants are made aware of this policy and the agreement as part of their induction
- Ensure regular information and education sessions are help for students and parents to promote understanding of available technologies, the inherent risks in volved in the use of those technologies and the content of the Acceptable Use Policy

6.2 Responsibilities of College Staff and Workplace Participants

College staff and workplace participants are required to:

- Educate students about the use of technology and the inherent risks involved in that use, including the potential inaccuracy of online information, ways to check authenticity of information, appropriate use of AI technologies, academic integrity, and strategies to stay safe online
- Work with the College Leadership to implement the ICT Acceptable Use Policy
- Promptly report to College Leadership, any known or suspected breaches of the College's Acceptable Use Policy and Acceptable Use Agreement that may constitute a criminal offence or require further investigation
- When using any device that accesses material on the SFdS network and services, only obtain access to records or information that is relevant to their duties, roles and responsibilities and that they have been authorised to access
- Promptly report to SFdS Leadership any loss of, or unauthorised access to, any ICT devices that contain work-related information or information that is otherwise confidential to SFdS or any unauthorised access to the College network itself
- Upon conclusion of their role within SFdS, permanently remove from their personal devices any work-related information, or information that is otherwise confidential to SFdS

- Employees and Workplace Participants must not:
  - Connect or interact with students through Social Media without the Principal's written consent, other than in the case of any Social Media site specifically created or provided by the College (and authorised by the Principal) for the purpose of facilitating online communication between employees, workplace participants and students (and/or parents)
  - Divulge any confidential information, including student personal information
- Employees and Workplace Participants' use of SFdS ict Facilities (including Personal ICT devices that are used to access materials on the College's network and services) may be monitored by SFdS ICT personnel, and any evidence of use that contravenes this policy, or is otherwise inappropriate, may lead to disciplinary action in accordance with the South Australian Catholic Schools Enterprise Agreement 2020. In the case of an investigation into the conduct of an employee or workplace participant, they must, if requested, provide their Personal ICT devices to SFdS Leadership (together with any information such as passwords that is necessary to gain full access to the devices) for the purposes of assisting the authorities to determine whether inappropriate conduct has occurred

7. Consequences of Non-Compliance

If a student is found to have breached the Acceptable Use Policy or Acceptable Use Agreement, consequences that may result will be in accordance with the Personal Responsibility Policy

If an employee or workplace participant is found to have breached the Acceptable Use Policy or Acceptable Use Agreement, consequences may include:

- Verbal counselling or warning
- Written counselling or warning
- Formal final warning
- Dismissal

Evidence of illegal conduct by students, employees or workplace participants will be reported to SAPOL or the Australian Federal Police, as appropriate.

LIMITATION OF LIABILITY

The terms of this document are not intended to be exhaustive, nor do they anticipate every possible use of SFdS's ICT facilities and services. Students, employees and workplace participants are required to act responsibly and take into account the principles underlying this ICT Acceptable Use Policy.

The College does not guarantee that the functions or services provided by or through its ICT resources will be error-free or without defect.

The College will not be responsible for any damage users or others may suffer including, but not limited to, loss of data or interruptions of service, whether or not such loss of data or interruptions of service is incurred through a breach of this Policy.

The College is not responsible for the accuracy or quality of the information obtained through, or stored on, College systems.

The College will not be held responsible for any financial loss or obligations arising through the unauthorised use of provided technology, nor for use breaching this policy or College ICT agreements.

DEFINITIONS

SFdS ICT Facilities and Services refers to Information and Communication Technologies and includes the provision of hardware, software and access to the Internet. This may include and is not limited to desktop, laptop, tablet computers, computer servers, electronic storage devices, network and telecommunications equipment and all associated software and all supporting peripheral devices.

Social Media refers to any internet or intranet website, program, tool or other electronic communication that publishes, posts, shares or discusses information, or allows interaction with others.

Cyberbullying is the use of the internet and related technologies to harm other people, or their reputation, in a deliberate, repeated and hostile manner.

Defamation refers to any statement (including photographs, media and animations) that can harm another person’s reputation.

Plagiarism is taking the ideas or writings of others and presenting them as if they were your own.

Copyright Infringement occurs when there is an unauthorised reproduction of a work that is protected by copyright.

Personal information means information or an opinion, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. The Privacy Act requires individuals and the College to take reasonable steps to protect the personal information that is held from misuse and unauthorised access.

SFdS refers to St Francis de Sales College

Workplace participants means consultants, contractors, volunteers and guests of St Francis de Sales College.

APPENDIX 1:

ASSOCIATED SACCS, CESA and OTHER SUPPORTING DOCUMENTS

CESA and SACCS ICT Acceptable Use Guidelines 1.01 (Version 1 2023)

SACCS Acceptable Use of Infrastructure and Communications Technology – Baseline Standard

CESA Social Media Guidelines

SFdS College Vison for Learning

SFdS Online Learning Guidelines

SFdS Policy on Academic Integrity and Assessment Deadline Procedure

SFdS Personal Responsibility Procedure

Protective Practices Guidelines (2019)

REFERENCES

eSafety: games, apps and social networking https://www.esafety.gov.au/key-issues/esafety-guide

Australian Federal Police ThinkUKnow: Cyber safety and security guide https://www.afp.gov.au/what-we-do/campaigns/thinkuknow

Melbourne Declaration on Educational Goals for Young Australians Melbourne Declaration on Educational Goals for Young Australians (curriculum.edu.au)

Alice Springs (Mparntwe) Education Declaration The Alice Springs (Mparntwe) Education Declaration - Department of Education, Australian Government