St Francis de Sales
COLLEGE

ICT, BYOD and Acceptable Use Policy

APPROVAL OF ICT, BYOD and Acceptable Use Policy

Principal:

College Board Chair:

Date:

Review Date:

CONTENTS

ICT, BYOD and Acceptable Use Policy (includes appropriate use of all Wireless Network Capable Digital Devices brought from home for school or class use).

SCOPE

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

Users include all full and part time staff, relief teachers, students, contractors, freelancers and other agents who use a personally owned, or school owned device to access, share, store, relocate or backup any school or student based data. Non-sanctioned use of personal devices to back up, store and otherwise access any data owned by the College and stored on our network is strictly prohibited.

Electronic and ICT Equipment and devices in this policy include, but are not limited to, computers (such as desktops, laptops & iPads), storage devices (such as USB and flash memory devices, CDs, DVDs, iPads, iPods, MP3 players and electronic books), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), and any other technologies as they come into use. This policy defines the standards, procedures and expectations for all users who are connecting a personally owned device to St Francis de Sales College's ICT network or who are using the College's ICT services, data and networks. The policy also applies to software and hardware that is not owned or supplied by the College, especially those that staff and students have acquired for personal use but are not licensed or formally approved by the College.

This Policy is to be read in accordance with the associated policies of CESA and the College, with specific reference to those in Appendix 1.

RATIONALE

Technology provides students and staff with unique and powerful ways to enhance their learning. St Francis de Sales College supports a learning environment where personalised learning and achievement is enhanced through appropriate and effective access to the tools and resources essential to achieving academic excellence. The College will continue to develop and evaluate Cyber Safety and e-learning practices which are directed and guided by this ICT, BYOD and Acceptable Use Policy and the College Personal Responsibility Policy.

New technologies play a particularly important role in enabling learning to occur beyond the boundaries of the school. Young people's familiarity with modern technology, and their engagement in e-learning, enhances curriculum-based learning and networking that extends around the world.

Mobile technologies, chat, blogs, wikis, webcams, reality television and interactive games are intrinsic to their worlds. Current technologies shape their expectations and their abilities to access, acquire, manipulate, construct, create and communicate information.

ICT capabilities and digital literacy are essential skills. The use of ICT will make significant gains for learners across all ages and curriculum areas.

Currently iPads and College recommended laptops are preferred devices due to their compatibility with the school wireless systems and their inbuilt protections against Malware. Devices from other manufacturers can be assessed for suitability by the school's ICT Coordinator, as some devices will have limited access to the College ICT networks and services.

Access to the College ICT networks, infrastructure and data is a privilege and all staff, parents, students and other persons seeking access to the College network must consent to and sign this BYOD policy prior to connecting the device to the College network.

Whilst acknowledging the role of ICT tools and services it is essential that we protect the integrity, confidentiality, security and confidentiality of all school data and that all employees and students act in accordance with our College policies to ensure that we minimise the risks of the following potential threats:

Threat	**Potential risk**
Device loss	Devices need to be password protected to minimise the loss or theft of work files
Data theft	Users need to ensure that sensitive College and student data are not uploaded onto devices, where they may be assessed by an unsanctioned third party
Malware	Viruses, Trojans, worms, spyware and other threats are increasingly a risk to our network where personal devices are not adequately protected from malware
Compliance	Loss or theft of personal or confidential data could expose the College to risk of non-compliance with various child protection, identity theft and privacy laws, so employees and students need to maintain compliance with this and related policies at all times

DEVICES CONNECTED TO THE COLLEGE NETWORK

The Principal of St Francis de Sales College retains the right to be the final arbitrator of what is, and is not, appropriate content and has overall responsibility for the appropriate access to and use of the College's ICT infrastructure, network and data management, including the right to monitor, access and review all use of College resources and infrastructure. This includes all personal web browsing, and emails sent and received on the College's ICT facilities.

As part of its quality assurance, data integrity and security processes, the College will establish audit trails capable of tracking the attachment of an external device to the College network in cases of suspected breaches of this policy or misuse of the College's ICT resources.

The College Principal also reserves the right to audit privately owned ICT electronic devices and equipment (including USBs) used on the College site or at any College related activity, to ensure the College ICT for Personal Learning and Acceptable Use Policy and Procedures are upheld at all times.

Connectivity of all staff and student owned devices will be centrally managed by the St Francis de Sales College IT Department, and configurations will be in accordance with the guidelines in place to protect and secure College data and information systems and storage. Configuration of devices will include password protection and encryption, and any other controls essential to isolating and protecting sensitive information accessed from or stored upon personal devices or the College network. Staff and students will be expected to adhere to the same security protocols when connected to non-school equipment to help protect any information from being lost or stolen from their devices.

No student, staff member or relief teacher is to divulge their password to a third party and all personal device users are responsible for bringing their devices to school fully charged and labelled for identification.

At the conclusion of a user's employment or enrolment at the College, all confidential school data, access privileges and email communication will be wiped from the personal device.

ACCEPTABLE USE

It is the responsibility of every student and employee of St Francis de Sales College to ensure that our ICT resources are never used to abuse, vilify, defame, harass, degrade or discriminate against others in line with the College's Personal Responsibility Policy. Thus all personal devices must be utilised responsibly, ethically and securely to safeguard the rights of others.

Thus, the following access controls must be observed at all times:

1. Personal devices will only be connected to the College network once the BYOD Registration form is completed and lodged.
2. Only registered devices will be permitted to access the College network and be connected to College data and resources, and must be used only for legitimate educational purposes.
3. All workplace users must employ reasonable security measures including, but not limited to, passwords, encryption, physical controls and safe storage of personal devices whenever they contain College data. Any attempt to contravene or bypass security or acceptable use procedures will be deemed a contravention of this ICT, BYOD and Acceptable Use Policy.
4. All workplace users must agree to only view, listen to, or access, school-appropriate content on their personal devices while at school and ensure that inappropriate material is not cached on any device being brought onto the College site.
5. Due to copyright, content such as music and games is not to be transferred to other devices or the school's computer network. Furthermore, students and staff may not use an audio recording device, video camera, or camera, or any device with one of these, to record media or take photos during school unless they have permission from the College and those whom they are recording.

Breaches of the College's ICT, BYOD and Acceptable Use Policy, will be responded to with consequences commensurate with the nature of the breach, but inevitably will involve exclusion from access to the College network for a period of time.

TERMS AND CONDITIONS

Examples of inappropriate use that will result in consequences to a user's access and privileges as outlined in the College's Personal Responsibility Procedures include any activities:

- that create security and/or safety issues for the College network, users, school or computer resources;
- that expend College resources on content it determines lacks legitimate educational content/purpose; or
- other activities as determined by St Francis de Sales College as inappropriate.

Such activities include but are not limited to:

1. Violating any St Francis de Sales or SACCS policies, state or federal law, such as: accessing or transmitting pornography of any kind, obscene depictions, and harmful materials, materials that encourage others to violate the law, confidential information, privacy requirements or copyrighted materials.
2. Criminal activities that can be punished under law.
3. Selling or purchasing illegal items or substances.
4. Obtaining and/or using anonymous email sites, spamming.
5. Causing harm to others or damage to their property.
6. Using profane, abusive, or impolite language; threatening, harassing, or making damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
7. Deleting, copying, modifying, or forging other users' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.
8. Damaging computer equipment, files, data or the network in any way, including intentionally accessing, transmitting or downloading computer viruses or other harmful files or programs, or disrupting any computer system performance.
9. Using any computer/mobile devices to pursue "hacking," internal or external to the College, or attempting to access information protected by privacy laws.
10. Accessing, transmitting or downloading large files, including "chain letters" or any type of "pyramid schemes."
11. Intentionally accessing, creating, storing or transmitting material that may be deemed to be offensive, indecent, obscene, racist, intimidating, or hostile; or that harasses, insults or attacks others.
12. Breaking copyright laws.
13. Attempting to use the network for non-academic related bandwidth intensive activities such as network games or transmission of large audio/video files or serving as a host for such activities

INSURANCE AND LIABILITY

The College does not accept liability for any loss, damage or theft of any BYOD device that is brought to school under the program. The responsibility for the storage, safe-keeping and care of the device is the responsibility of the device owner. The College insurance policy does not apply to these devices; instead these are covered by the user's insurance policy. As such it is strongly recommended that families ensure that the details such as serial numbers and receipts of purchase for these devices are stored securely at home for insurance purposes.

APPENDIX 1

ASSOCIATED SACCS AND OTHER DOCUMENTS

- South Australian Commission for Catholic Schools Vision Statement 1991 and reprinted 1996 https://online.cesa.catholic.edu.au/docushare/dsweb/Get/Document-19939/CESA+-+Mission+Values+and+Vision+Revised+version+July+2012.pdf

- Communications Technology Policy (containing acceptable use section) Home CESA Services Policies, Procedures & Guidelines

- CESA Strategic Plan http://online.cesanet.adl.catholic.edu.au/docushare/dsweb/Get/Document-13434

- SACCS ICT Security Policy 2007 http://online.cesanet.adl.catholic.edu.au/docushare/dsweb/Get/Document-8998/ICT+Security+Policy+1-00.pdf

- South Australian Catholic Child Protection Council Implementation Guidelines for the Care, Wellbeing and Protection of Children and Young People (Contact the CEO for further details 83016600)

- Policy for the Care, Wellbeing and Protection of Children and Young People 2009 http://online.cesanet.adl.catholic.edu.au/docushare/dsweb/Get/Document-13163/Policy+for+the+Care+Wellbeing+and+Protection+of+Children+and+Young+People+18+November+final.pdf

- Child Protection Curriculum, Teacher Support Module for SA Catholic Schools, CEO 2009 (Contact the CEO for further details 83016600)

- 'Protective Practices for Staff in their Interactions with Students – Guidelines for Schools, Preschools and Out of School Hours Care' DECS, CEO and AISSA 2009 https://online.cesa.catholic.edu.au/docushare/dsweb/Get/Document-29723/Protective+practices+for+staff+in+their+interactions+with+children+and+young+people+2017.pdf