ICT Policy for Personal Learning and Acceptable Use
(includes personally owned learning devices)

APPROVAL OF ICT POLICY FOR PERSONAL LEARNING

Principal: [Signature]

College Board Chair: [Signature]

Date: 25 January 2013

Review Date: 25 January 2014
CONTENTS

PURPOSE ........................................................................................................................................... 4

RATIONALE ......................................................................................................................................... 4

MONITORING OF DEVICES CONNECTED TO THE COLLEGE NETWORK ....................................... 5

TERMS AND CONDITIONS .................................................................................................................. 7

INSURANCE AND LIABILITY ............................................................................................................. 8

YEAR 6-12 STUDENT AGREEMENT .................................................................................................. 9

YEAR 6-12 CONSEQUENCES .............................................................................................................. 10

RECEPTION – YEAR 2 STUDENT AGREEMENT ............................................................................. 11

YEAR 3-5 STUDENT AGREEMENT .................................................................................................... 12

RECEPTION – YEAR 5 CONSEQUENCES ............................................................................................ 13

APPENDIX 1: ASSOCIATED SACCS AND OTHER DOCUMENTS .................................................... 14

APPENDIX 2: CLOUD COMPUTING SERVICES USER AGREEMENT - STUDENTS ............................. 16
BYOD - ICT Policy for personal learning (includes appropriate use of all Wireless Network Capable Digital Devices brought from home for school or class use).

PURPOSE
This policy defines the standards, procedures and expectations for all users who are connecting a personally owned device to St Francis de Sales College 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.

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. 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 may be allowed by the school’s ICT Coordinator, after assessment for compatibility and, where required, assessment of up to date anti-virus protection. All other 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. 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 back up 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.

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 for Personal Learning and Acceptable Use Policy and the College Cyber Safety and Personal Responsibility policies.

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.
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:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Potential risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device loss</td>
<td>Devices need to be password protected to minimise the loss or theft of work files</td>
</tr>
<tr>
<td>Data theft</td>
<td>Users need to ensure that sensitive corporate data is not uploaded onto devices and stolen or sold by an employee or unsanctioned third party</td>
</tr>
<tr>
<td>Malware</td>
<td>Viruses, Trojans, worms, spyware and other threats are increasingly a risk to our network where personal devices are not adequately protected from malware</td>
</tr>
<tr>
<td>Compliance</td>
<td>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</td>
</tr>
</tbody>
</table>

**MONITORING OF 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. Such tracking will be able to monitor dates, times and duration of access to ensure that College data and security has not been compromised by external parties.

Consequences for breach of this policy will be determined by the Principal and may include banning an individual from bringing their mobile device to school. The College Principal also reserves the right to audit at any time any material on equipment that is owned or leased by the College, and 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.
Failure to comply will result in immediate suspension of all network access privileges so as to protect the College’s infrastructure. 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.

Any phone internet connection, such as 3G, YesG or NextG, must be switched off if possible and the device priority pointed to the school’s wireless network. Accessing the internet independently of the school’s proxy servers (ie by personal ISP) is not allowed in order to ensure cyber safety.

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

**ICT for Personal Learning and Acceptable Use Policy**

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. Thus all personal devices must be utilised responsibly, ethically and securely to safeguard the rights of others and the security of all College data, ICT systems and infrastructure.

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

1. The College IT Services Team reserves the right to refuse the connection of personal devices to the College network if such equipment is being used in any way that could potentially cause harm to the Colleges’ systems, data, users or resources.

2. Only appropriately managed and registered devices will be permitted to access the College network and be connected to College data and resources. Such devices must adhere to the College’s authentication requirements at all times.

3. All 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 for Personal Learning and Acceptable Use Policy and will limit the ability of the user to access the College’s ICT network and resources.

4. Staff and students agree to only view, listen to, or access, school appropriate content on their personal devices while at school.

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, e.g. cell phone, laptop, tablet, etc.) to record media or take photos during school unless they have permission from the College and those whom they are recording.

6. **Mobile phone photos, voice and text use by students during the school day are prohibited by this policy.**

**TERMS AND CONDITIONS**

Examples of inappropriate use that will result in termination of a user’s access and privileges 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 state or federal law or municipal ordinance, such as: accessing or transmitting pornography of any kind, obscene depictions, and harmful materials, materials that encourage others to violate the law, confidential information 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, spreading viruses.

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, intimidating, or hostile; or that harasses, insults or attacks others.


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 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.
YEAR 6 - 12 STUDENT AGREEMENT

The safety of the students of St Francis de Sales College is of paramount concern. Any apparent breach of Cyber Safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the College’s Personal Responsibility Policy in regard to Cyber Safety practices. In serious incidents, advice will be sought from appropriate external sources, such as the police, NetSafe and/or a lawyer with specialist knowledge in this area. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

Students may not use the College’s Internet facilities and ICT resources in any circumstances unless the appropriate BYOD and Acceptable Use Agreement has been signed and returned to the College. Online resources for parents and students include www.wiseuptoit.com.au and www.netalert.gov.au

The specific conditions of the User Agreement are outlined below.

I understand that the use of ICT equipment and access to the Internet at St Francis de Sales College must be in support of educational research and learning. I take sole responsibility for use of my accounts and passwords and personally owned devices and will not share my password with others.

I will refrain from accessing any websites, images, computer files, newsgroups, chat groups or other electronic material from any sources that would be considered offensive in the judgement of the College.

I will be courteous and use appropriate language in communication via the Internet. I will refrain from using obscene, harassing or abusive language and will report any occurrences of such usage against me to a teacher, or a member of staff. I will ensure that I do not use ICT resources to abuse, vilify, defame, harass, degrade or discriminate others.

I accept responsibility in regard to copyright protected material. Therefore, I will not download and redistribute software, games, music, graphics, videos or text unless authorised to do so by the copyright owner and/or the College.

I understand that plagiarism (presenting someone else’s work as my own) is unacceptable. Therefore, I will list any downloaded material used in the preparation of assignments in a bibliography and clearly indicate where material has been directly quoted from another source.

I will not reveal personal details of myself or others via ICT resources unless instructed to do so by the College.

I shall not maliciously destroy or steal ICT equipment from the College. Unacceptable or rough use of any equipment belonging to the College, myself or other students or staff will also not be tolerated. If I have damaged ICT equipment I understand that the costs for repair or replacement will be me and my parents’ responsibility.
I understand that I am never permitted to use the College network for private storage for non-educational, non-approved files, including games, videos, music, etc.

If I violate any of the terms of this agreement, I will be subject to the consequences outlined below.

**YEAR 6-12 CONSEQUENCES**

The following are consequences for breaches of the BYOD and Acceptable Use Policy:

1. Warning from subject teacher and note in diary which needs to be signed by both the Homeroom teacher and the parent. Repeat offences may incur significant penalties including limited or no access to the College ICT network and related sources.

2. Student blocked from computer use for a total of 5 school days (excluding days where students are not in the classroom). Head of School to send letter home informing parents of this serious consequence. (Students are still expected to complete all school work on time.)

3. In circumstances, which involve harassment, accessing inappropriate material or materials that compromise or attempt to compromise the College’s network, students will be automatically blocked for a 5 day period or until ethical and legal compliance issues have been resolved.

4. When a student is found to have maliciously damaged equipment, they will be blocked from computer use for a 10-day period; unacceptable or rough use of the equipment will also not be tolerated. Any damaged equipment may have costs recovered for repair or replacement by the student/parents who are responsible for the damaged equipment.

5. Students, who fail to comply with the policy guidelines and procedures for personally owned devices, will have their access and connectivity privileges suspended until compliance is guaranteed by the student and family.

6. Students who damage or misuse others’ personally owned devices will be responsible for any replacement or repair costs associated with such damage or theft.
RECEPTION - YEAR 2 STUDENT AGREEMENT

As an iPad user at St Francis de Sales College I agree to abide by the following rules and expectations. I understand that if I choose not to follow these rules I must be prepared to accept the consequences.

I will be responsible for my own and the school iPads by:
• Keeping my iPad in a safe box in the classroom until I am asked to get it
• Keeping my iPad in the middle of my desk or in a safe place on my desk
• Keeping my water bottle under my desk
• Always using 2 hands when carrying an iPad
• Always keeping the iPad in its cover
• Always walking when carrying an iPad
• All iPads stay in the classroom at recess and lunch
• Never touching anyone else’s iPad
• Keeping my iPad in my bag when travelling to and from school AND keeping my bag zipped up.
• Not playing with my iPad before and after school and on the bus
• Making sure my iPad is charged each day
• Having clean hands when using any iPad

I will learn best from using an iPad in the classroom by:
• Only using the apps the teacher asks me to use
• Not playing games from home in the classroom
• Listening carefully and following instructions
• Only using internet sites that I need for my learning when the teacher asks me to

I will use the iPads responsibly and safely by:
• Always having my screen visible at school and home
• Only accessing the websites the teacher asks me to
• Reporting anything I see that is inappropriate or makes me feel uncomfortable straight away to the teacher
• Never taking photos or video of anyone without their permission or teacher approval
• Never giving out personal information online
• Keeping my password secret and only ever using my own password
• Thinking before I act!
YEAR 3-5 STUDENT AGREEMENT

As a computer user of St Francis de Sales College, I will follow these rules:

- I will only use the ICT equipment for educational or approved class-based purposes.
- I will take care of the College’s hardware and software.
- I will be responsible for my own iPad or other mobile electronic device.
- I will only use resources, software and apps that have been approved by the teacher.
- I understand the use of the Internet and email is a privilege.
- I will keep my password private and not use the passwords of others.
- I will not pretend to be someone else or disguise my identity when accessing online communities.
- I will not give out personal information such as name, address, and phone number of myself or others.
- I will access the Internet for resources that are relevant to my school work.
- I will not download material without teacher approval.
- I will not deliberately access inappropriate or offensive material. If I accidentally come across something that is inappropriate and possibly breaches the ICT agreement, I will immediately close the application I am using or leave the internet site and inform the teacher.
- I will not record pictures, video or audio of anybody without first getting permission from that person and the teacher.
- I will not publish pictures, video or audio of myself or others without teacher approval.
- I will be respectful and use appropriate written expression as expected by the College in all communication.
- All mobile electronic devices will only be used with the teacher’s permission.
- I understand that the College may check and audit any electronic devices I bring into the College, any files stored on the College network and may monitor the Internet sites I visit.
- I will not bring games, music and inappropriate material from home and place them on the College’s network.
- I will not interfere with any computer security measures the College may have in place.
- I will not attempt to access files belonging to others.

Online resources for parents and students on safe use of the Internet can be found at [cybersmart.gov.au](http://cybersmart.gov.au)

A very useful resource for online learning and living is also to be found at [www.forwardit.sa.gov.au](http://www.forwardit.sa.gov.au)
RECEPTION – YEAR 5 CONSEQUENCES

The safety of the students of St Francis de Sales College is of paramount concern. Any apparent breach of Cyber Safety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the College’s Personal Responsibility Policy in regard to Cyber Safety practices. In serious incidents, advice will be sought from appropriate external sources, such as the police, NetSafe and/or a lawyer with specialist knowledge in this area. If illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency. Reference: www.netalert.gov.au

In the event of inappropriate use of the computer the following will occur:

**Step 1.** Warning from class teacher.

**Step 2.** Re-negotiating of ICT agreement with class teacher and/or Head of School.

**Step 3.** Removal of access to computers for a negotiated period of time.

Students will go directly to Step 3 in circumstances that involve:

- Harassment / Bullying
- Accessing inappropriate material
- Altering or compromising the College’s network

**Damage to ICT equipment.**

Student’s access will be removed for a negotiated period of time and with parent notification.

**NB.** The above inappropriate use and consequences could also be covered by other College policies. When a student has damaged computing or other equipment, the parents will be notified and will be responsible for replacing/repairing the equipment.
APPENDIX 1

ASSOCIATED SACCS AND OTHER DOCUMENTS


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

- CESA Strategic Plan

- CESA ICT Strategic Plan Template
  http://online.cesanet.adl.catholic.edu.au/docushare/dsweb/View/Collection-2536


- South Australian Catholic Child Protection Council Charter

- South Australian Catholic Child Protection Council Policy for the Care, Wellbeing and Protection of Children and Young People, 2006

- 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

- South Australian Commission for Catholic Schools, Duty of Care Policy 2004

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

• Keeping Safe: Child Protection Curriculum, DECS, 2008

• ‘Protective Practices for Staff in their Interactions with Students – Guidelines for Schools,
  Preschools and Out of School Hours Care’ DECS, CEO and AISSA 2009
  http://online.cesanet.adl.catholic.edu.au/docushare/dsweb/Get/Document-
  6076/Protective+Practices+edited+April+2009+version.pdf

• Information Sharing: Guidelines for Promoting the Safety and Wellbeing of Children, Young
  People and their Families, Govt of SA

• National Safe Schools Framework,

Child Wise, Choose with Care, Building Safe Organisations http://childwise.net/
This User Agreement sets out the terms on which you may access cloud computing services provided by the school, including Google Apps and Edublogs (Cloud Computing Services). Cloud computing involves the use of web-based services (rather than a PC or school server) for functions such as email, blogs and data storage.

You will need to sign and return this User Agreement before you will be allowed to access the Cloud Computing Services.

By signing this User Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

1. Privacy Consent
Information that you transfer or store using the school’s Cloud Computing Services (including email, blogs and data storage) may be stored by Google, Edublogs or other Cloud Computing Service providers (Cloud Providers) in the United States of America, or such other country as the Cloud Providers may decide. By using the school’s Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

2. Acceptable Use
You agree that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

(a) give your account password to anyone else;

(b) access (or try to access) anyone else’s account, or try to defeat any security controls;

(c) send or help to send unsolicited bulk email (spam);

(d) publish, send or knowingly access material that is pornographic, hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;

(e) knowingly create or send any viruses, worms, Trojan horses or anything of a similar nature; or

(f) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

3. Monitoring
You agree that school staff and Catholic Education Office staff responsible for ICT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including
accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

If you notice a problem with the Cloud Computing Services, or if you think that someone is trying to access your account (or someone else’s account), you agree that you will tell the school ICT Coordinator straight away.

4. Suspension or termination of use and other consequences

If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school’s ICT services, including your school email account. If you are found to have made inappropriate use of the Cloud Computing Services, the school may also apply other disciplinary consequences.