

# **INFORMATION & COMMUNICATION TECHNOLOGY POLICY**



**St Francis Xavier College  
Berwick, Beaconsfield & Officer  
Ratified by Board of Management  
October, 2001  
Amended June, 2005  
Ratified by College Board September, 2005  
Amended September, 2008  
Ratified by College Board October, 2008  
Amended November 2011  
Ratified by College Board November 2011**

## VISION AND MISSION STATEMENT

*St. Francis Xavier College is a Catholic community that is educative and supportive. We have a clear purpose: the development of a person of competence, conscience and compassion formed in the Christian tradition; one who is guided by a sense of hope and self-belief and who will be of service in the world. We recognise God's presence in our lives by celebrating and pursuing personal excellence and by living courageously with optimism and respect for all.*

### WHAT IS INFORMATION AND COMMUNICATION TECHNOLOGY?

Information and Communications Technology (ICT) is an umbrella term that includes all technologies for the manipulation and communication of information. ICT encompasses any medium to record information (magnetic disk/tape, optical disks (CD/DVD), flash memory, etc. and arguably also paper records); technology for broadcasting information - radio, television; and technology for communicating through voice and sound or images - microphone, camera, loudspeaker, telephone to mobile phones. It includes the wide variety of computing hardware (PCs, servers, mainframes, networked storage); personal hardware, including but not limited to, mobile phones, BlackBerry, MP3 players. Thus, ICT makes more explicit that technologies such as broadcasting and wireless mobile telecommunications are included.

Information and Communication Technology prepares students to participate in a rapidly changing world in which work and other activities are increasingly transformed by access to varied and developing technology. Students use ICT tools to find, explore, analyse, exchange and present information responsibly, creatively and with discernment. They learn how to employ ICT to enable rapid access to ideas and experiences from a wide range of people, communities and cultures. Increased capability in the use of ICT promotes initiative and independent learning; with students being able to make informed judgements about when and where to use ICT to best effect, and to consider its implications for home and work both now and in the future.

### RATIONALE

St Francis Xavier College recognises and values the role of ICT in

- enhancing the teaching and learning process in all subjects;
- developing literacy, numeracy, communication, problem solving, information handling, social, interpersonal and independent learning skills among pupils;
- encouraging students to experiment, explore, understand, interpret, research, select, present, check and improve their work
- enabling students to test hypotheses, create conceptual models and improve decision-making;
- responding to the requirements of the Victorian Essential Learning Standards (VELS), the Victorian Certificate of Applied Learning (VCAL) and Vocational Education and Training (VET).

### STATEMENT OF INTENT

This policy document sets out the College's aims, principles and strategies for the delivery of Information and Communication Technology.

The Catholic Network Australia (CNA) will provide network infrastructure to assist all Australian Catholic Church agencies and organisations to provide more sophisticated services in the future. The College connects to this network.

The College will strive to achieve and maintain a student to computer ratio of 3:1. Computers and monitors will be replaced every 3 years; all other hardware will be replaced every 4 years, so that no piece of hardware is older than 4 years.

## **LEARNING TECHNOLOGIES COMMITTEE (LTC)**

At St Francis Xavier College, appropriate use of ICT is the responsibility of all staff. However, the **College Executive**, the senior leadership team, oversees all ICT matters, and is advised by the Learning Technologies Committee which is chaired by the Director of Innovation (eLearning).

### **Members of the Learning Technology Committee are:**

- Director of Innovation (eLearning) – Chair
- Business Manager
- ICT Manager
- Senior AV Technician
- Directors of Learning
- Staff representatives from across the curriculum
- Staff as required

Among other duties, the LTC will

- Recommend personnel and other resources to assist the school in developing and achieving its learning technology plan.
- Recommend appropriate and ongoing professional development for teachers and administration staff with respect to leadership and management of learning technologies and developing skills, knowledge and attitudes to enable schools to use learning technologies and create digital resources.
- Develop and support mechanisms for consultation and collaboration with other schools with regard to this policy.
- Develop and support cooperative arrangements for ongoing support and maintenance of schools' networks.
- Review the ICT Policy.

## **ACCESS and USE**

Access to the network and the Internet is obtained through computer hardware located in designated classrooms, libraries, computer rooms and laptop stations. Staff may also use computer equipment located in offices and staffrooms.

An account, allowing access to various facilities and the Internet, is issued to each student and staff member with the understanding that they will abide by the guidelines and rules contained in the ICT Policy and all College regulations.

By logging onto the network, users are formally acknowledging their understanding of this policy and its guidelines as a condition of using the network or receiving a personal account. Students are further required to complete the ICT Declaration of Acceptance in the Student's Handbook. Students are required to complete this form again as part of the re-commitment process.

All persons using the computer network have a responsibility to ensure the correct and proper use of the computer network.

- **Role of Technician**

The College ICT technicians are responsible for the maintenance of the College computer networks. They undertake the role of Systems Administrators. This includes routine scans of the network, upgrades to servers and computers, conducting repairs as appropriate, purchasing hardware and software for the College, etc. They are also required to assist teaching staff where possible. The ICT Technicians are not permitted to undertake repairs on the personal computers of staff and students. For a full description of the duties of the ICT technicians refer to the position statement.

- **Role of Teachers**

Teachers should use the College ICT equipment for educational purposes either in the classroom to enhance student learning or for lesson preparation. Teachers have

the responsibility to update their ICT skills and to keep up to date with current practice. Teachers are not permitted to allow students to use their (teachers') accounts. Teachers must be vigilant at all times to ensure appropriate use of ICT.

- **Role of Non-Teaching Staff**

Non-Teaching staff may use the computer network **ONLY** to complete their daily functions within the college.

- **Role of Students**

Students are permitted to use the College ICT equipment to complete school work set by teachers, and/or for purposes of educational research only. They can access the network from computer rooms, computer pods, library or another specialist location. Students must abide by the conditions of acceptable use as described in the ICT Policy.

### **Software**

All software that is used on the College computer network must be purchased by the ICT Manager and approved for technical suitability. Before being loaded onto the College computer network ICT technicians will make a backup copy of the software and store it securely. If any software needs to be accessed by any member of staff it needs to be borrowed from and returned to the ICT technicians.

### **College Network**

All users (students & staff) are supplied with their own unique login names and passwords. An identical login name is allocated for access to the Internet by the Internet Service Provider. In the case of duplicate names the ICT Technicians will decide on the best course of action. Access to this network is gained through computer hardware located in designated classrooms, library, computer rooms and computer pods. Staff may also use computer equipment located in offices and staffrooms. Users of this network are not permitted to allow another person to use their logon account.

Both Networks have access to the Internet. The purpose of the Internet is to facilitate communications in support of research and education. As part of this connection each user is supplied with an e-mail account.

Students and staff also have access to digital scanning equipment, a digital camera, and digital video editing equipment. Students are allocated secure personal home directories (workspace on the network) that may be used to save their work. The ICT Technicians will determine the amount of space allocated to each user based upon needs and availability of network resources. This amount must not be exceeded unless the Systems Administrator gives special permission to do so. Material that the Systems Administrator deems as inappropriate must not be saved on College computer equipment. This includes, but is not limited to, games, executable file, Music files, zip files, mpeg files and some picture files.

## **ACCEPTABLE USE**

The following terms and conditions for the acceptable use of ICT equipment at the College apply to all users and networks.

### **Network**

No student is permitted access to an IT classroom unless under the direct supervision of a teacher, who must remain in the room at all times. Similarly no student is permitted to remain in the room after class unless the teacher remains in the room to supervise the student.

During the course of network logon session students must not:

- Move around unnecessarily.
- Remove, damage or attempt to repair any component of the Network.
- Bring or consume food or drink in a computer room or pod,
- Through direct action cause damage to the computer network.

## ST FRANCIS XAVIER COLLEGE

- Install any software onto the computer hardware.
- Download any software or applications even if they are not stored on the College network.
- Attempt to access secured parts of the network.
- Connect non St Francis Xavier hardware to the computer network including, but not limited to, laptops, personal computers and portable hard drives above 4GB
- Use another user's account including students and teachers to access the computer network.

During the course of network logon session, students must:

- Immediately report any and all problems with the College Computer Network to the classroom teacher.
- Demonstrate appropriate respect for property.
- Use only those applications that apply directly to current work.
- Ensure that any removable media device used on the network is virus free.

At the conclusion of lessons in the computer rooms and pods, students must:

- Leave the computer room or pod in a tidy state.
- Ensure that all computers are logged off and reset and that the area around their workstation is tidy.

At the conclusion of each lesson in a computer room or pod teachers must:

- As soon as is reasonably possible, report any faults.
- Not allow any student to undertake repairs to the Network.
- Ensure that all computers are logged off and reset and that the room is tidy.

During the course of the lesson teachers must:

- Not allow any student banned from the college network access to the network via temporary or other means.
- Move about the Computer room or Pod at all times and be fully aware of the actions of students in the classroom.
- Have read the ICT Policy and be aware of its contents.

All users have a responsibility to:

- Report any faults.
- Not disclose their password or logon details.
- Lock their workstation if leaving it unattended.
- Use the computer network only for work that is directly related to education or educational purposes.

### **Internet**

The College's Internet facilities must not be used to:

- Access, view, download, print, disseminate or post any material that may be considered inappropriate, offensive, defamatory, obscene, pornographic or discriminatory, including material that is sexually explicit or that has racist, sexist, discriminatory, political or religious content, or which includes inappropriate comments in relation to sexual orientation, disabilities or any other physical attributes. This list is not exhaustive.
- Attempt to probe security mechanisms at the College or any other Internet sites.
- Post any information on Internet news groups, bulletin boards or similar forums on behalf of the College unless specifically authorised to do so.
- List information from articles on the Internet – unless the Computer User has adhered to the same protocols for recognising source information that apply to the use of hard copy documents as reference or research material.

During the course of network Internet session, students must not:

- Download any program.
- Play online games.
- Access any streaming media.

## ST FRANCIS XAVIER COLLEGE

- Knowingly download a virus or similar program that will cause damage to the computer network.

### **Electronic-mail (e-mail)**

The e-mail system may be used only for school purposes.

Users of the College's e-mail system must not use it:

- In a way that may be considered offensive, defamatory, obscene, pornographic, discriminatory, insulting or disruptive to any other person (for example, pictures of naked people, semi clothed people, personal comments about colleagues, students or staff).
- To access, view, download, print or send messages or attachments (including to your home e-mail address), which include:
  - Language that is not appropriate including, but not limited to, swearing, sexually explicit references.
  - Sexually explicit messages or pictures.
  - Offensive or inappropriate cartoons or jokes.
  - Unwelcome propositions or love letters.
  - Ethnic or racial slurs.
- To access other people's e-mail accounts.
- For sending chain mail, gambling, participating in on-line games, retrieving games or screen savers unless there is a business need to do so, joining a mailing list or chat group, posting messages to news groups, or engaging in on-line purchasing or selling.
- To distribute the copyright material of third parties, including software, database files, documentation, pictures, articles, graphic files, text or other downloaded information.
- For intentional dissemination of any computer viruses.
- For personal advertising or for personal profit making.
- For distributing personal information (information or an opinion that can identify a person) about a person unless the person's consent is obtained.

The College understands that computer users cannot always control the messages that are sent to them. However, computer users must discourage third parties (such as family, friends or workmates) from sending inappropriate messages to them.

If a computer user receives an inappropriate message or attachment to an e-mail the user must:

- Send an e-mail to the person who sent the inappropriate e-mail which indicates that such messages should not be sent. An appropriate form of response would be:  
*'Please do not send me this type of material again. The contents of this e-mail do not comply with the College's electronic mail policy. In sending me this e-mail you are breaching the College's policies and putting me at risk of doing so. A breach of the electronic mail policy has serious consequences.'*
- Forward a copy of this response (together with the inappropriate e-mail) to the ICT Technicians.
- Delete the e-mail.

All users of the e-mail system have a responsibility to

- Ensure that they do not exceed the mail box size limit.

### **Laptops**

Teachers are permitted to bring laptops into the College, however, they will have limited access to College Network for security purposes.

All **Acceptable Use** terms and conditions apply to users who connect to the network or access the Internet using a laptop computer.

All supplied laptop computers remain the property of the College and as such the use of these machines are bound by the Information and Communication Technology Policy.

### **Removable media**

The College understands that removable media is necessary for use with computer data transfer and storage. Because they are attached to the computer network the following rules apply.

Users must:

- Ensure that all files are free of viruses.
- Accept responsibility for the maintenance of the device.

Users must not:

- Download inappropriate material to any removable media device as stated in the network, Internet and e-mail sections.
- Use the device for the storage of material that is prohibited by the ICT Policy.
- Use the device for accessing prohibited material.

### **Exceptions**

There are some circumstances where the above terms and conditions do not apply. These are as follows:

- **Library.**  
To use one of the workstations located in the Library, students must first book in at the loans desk. If a student from a timetabled class goes to the Library to use a computer s/he must have a note written in the student record book by the subject teacher which details the topic and/or purpose for use of the computer. All other terms and conditions apply
- **VCE Information Systems, VET Information Technology, VET Music, VET Multimedia.**  
These classes require students to use applications that produce executable files, which are not permitted under the ICT Policy. It is the subject teacher's responsibility to inform the ICT technicians of the students who are in these classes and the type of files that they may have. The ICT technicians will provide a location for storage of these files.

## **BREACHES OF ICT POLICY**

### **Students**

#### **Breach of Acceptable Use consequences**

##### **Minor Breach**

This includes but is not limited to playing games, downloading executable files, accessing inappropriate images, sending inappropriate e-mails.

- Ban from network, and disciplinary action as determined by Deputy Principal: Head of Campus

##### **Major Breach**

This includes, but is not limited to, hacking software and devices which damage the security of the network, and wilful damage to the network.

- Indefinite ban. Payment for repairs. Conference with parents. Disciplinary action as determined by Deputy Principal – Head of Campus. Activity which may be deemed to be criminal will be reported to the police.

##### **Warranty**

The College makes no warranties of any kind, whether expressed or implied, for the service it is providing. The College will not be responsible for any damage a user suffers. This includes,

but is not limited to, loss of data resulting from delays, non deliveries, missed deliveries, or service interruptions caused by the College, Vic One, the ISP, EduNet or SchoolsNet. Use of any information obtained via the Internet is at the user's own risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information, and consider how valid that information may be (reliability of source, accuracy, timeliness, completeness, etc).

## **YEAR 12 STUDENT PERSONAL DEVICE USAGE GUIDELINES**

### **INTRODUCTION**

To enhance the learning experience of its students, St. Francis Xavier College aims to provide students access to its Student Wireless Network and the option of utilising personally-owned devices. The purpose of these guidelines is to ensure that students and their parents recognise the limitations that the College imposes on the use of personally-owned devices when they are used at the College in conjunction with the wireless network.

These guidelines are supplemental to the St. Francis Xavier College Information and Communication Technology Policy and the ICT Policy Guidelines and Agreement. These guidelines and policies apply to the use of all laptop and netbook computers including iPADS.

### **COLLEGE GUIDELINES ON PERSONAL ELECTRONIC DEVICES**

#### **General Usage Guidelines**

- The College will not be held responsible in any capacity for physical damage, loss or theft of any personally-owned device.
- Student use of personally-owned devices in the classroom will be at the discretion of the classroom teacher. Classroom teachers may prohibit, restrict or regulate use of personally-owned devices as they deem necessary.
- Student use of a personally-owned device must support the instructional activities and educational aims currently occurring in the College environment.
- Students should be aware that the use of personal computing devices could cause distraction for others, especially in regards to audio. Therefore, audio must be muted or restricted with student owned headphones, earphones unless otherwise directed by a College authority.
- Student devices with camera and video capability must not be used to record the image or audio of any student or staff member without the express written permission of the College AND the individual concerned.
- Before school, at lunch and after school, students may use their personally-owned devices *only* for study purposes and in supervised areas such as the Library and Study Areas.
- By bringing, personally owned devices to the College, students and their families accept that College staff will inspect the device and its contents to ensure compliance with the St. Francis Xavier College Information and Communication Technology Policy and the ICT Policy Guidelines and Agreement.
- Students use the Student Wireless Network at their own risk. The College will not be held responsible for any damage that may occur as a result of connecting to the Student Wireless Network or any electrical power source. ICT will not be responsible for maintaining or trouble shooting software or hardware-related issues with personal electronic devices.
- The parents and/or guardians of any student bringing personal technology to the College are responsible for its use and will be required to reimburse the College for any damage that their child may cause through the use of Student Wireless Network with his/her personally-owned device.
- Students must not attempt to circumvent the restrictions imposed by the College network and must not give passwords or any other access codes or certificates gained under these guidelines.
- Students will be provided access to the internet only. Students will not have access to printers, their home directory (H: drive), or any other network services.

## ST FRANCIS XAVIER COLLEGE

- Students are not permitted to access the internet through mobile network devices (commonly known as 'dongles') that allow unfiltered access to the internet while on College premises.
- Students are expected to bring the device to school ensuring that it is charged and has enough power to last the day. The College will provide no provisions for students to charge and power their personal device on site.
- Technical support of personal devices is not provided by the College ICT Department.
- Unless notified by the Director of Learning (incorporating VCE) students are not permitted to use electronic devices for SAC/SAT school based examinations. Please refer to the 2011 VCAA Administration Handbook 11.2.3 – Management of programs for students requiring Special Provision – Provision of facilities and technology.

While the use of technology in learning strategies is encouraged, the use of new and emerging technologies in assessments should first be discussed with the VCAA, to avoid the possibility of the technology being disallowed for use in an examination as part of Special Examination Arrangements and therefore the coursework tasks. **The technology allowed for school-based assessment tasks should reflect those which the student will be allowed to use in an external examination.**"

### USAGE CONSEQUENCES

Failure to comply with these guidelines and policies may result in disciplinary action by the school which may include, but is not limited to, loss of access to the Student Wireless Network.

### REGISTERING YOUR PERSONAL ELECTRONIC DEVICE

To apply and register your Personal Electronic Device to be able to connect to the College Student Wireless Network students must successfully complete the following steps:

1. Complete the Personal Usage Device Agreement document which includes signatures from both the student and the parent acknowledging acceptance of the agreement.
2. Submit the form to the Deputy Principal – Head of Campus for their endorsement and signature approving the application. A St. Francis Xavier College approval sticker will be affixed to the device or the Student Record Book.
3. If such permission is granted, take a copy of the completed documentation and the Personal Electronic Device to the ICT Help Desk to receive instructions on how to connect to the Student Wireless Network.

*The following Student Personal Device Application and Acknowledgement Form is also an addition.*



### Student Personal Device Application and Acknowledgement Form

Student's Name: \_\_\_\_\_

Year Level: \_\_\_\_\_ Care Group: \_\_\_\_\_

#### Type of Personal Electronic Device:

Laptop

Netbook

IPAD

Manufacturer: \_\_\_\_\_

Model: \_\_\_\_\_ Serial No: \_\_\_\_\_

MAC Address: \_\_\_\_\_ ICT Use Only

#### Student Acknowledgement

I have read the Student Personal Device Usage Guidelines and accept the terms and conditions of the policy.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

#### Parent Acknowledgement

As the parent of \_\_\_\_\_, I have read I have read the Student Personal Device Usage Guidelines and accept the terms and conditions of the policy.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

#### Deputy Principal Approval

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

*Please submit this form to the Deputy Principal – Head of Campus for approval.*

## St Francis Xavier College – ICT Policy Guidelines

St Francis Xavier College provides to all students access to its computer network and Internet facilities. Each student has the responsibility to read and accept the rules and provisions that govern the use of this resource. The following is an incomplete list of the college's Computer network Acceptable Use Policy.

### Network

No student is permitted access to an ICT classroom unless under the direct supervision of a teacher,

During the course of network logon sessions students must not:

- Remove, damage or attempt to repair any component of the Network.
- Bring or consume food or drink in a computer room or pod.
- Through direct action cause damage to the computer network.
- Install or download any software or applications even if they are not stored on the network.
- Attempt to access secured parts of the network.
- Connect non St Francis Xavier hardware to the computer network including but not limited to laptops, personal computers and portable hard drives above 4GB.
- Use another user's account including students and teachers to access the computer network.
- Use the computer network for any purpose not directly related to school work.

During the course of network logon sessions, students must:

- Immediately report any and all problems to the classroom teacher.
- Demonstrate appropriate respect for property.
- Use only those applications that apply directly to current work.

### Internet

The College's Internet and electronic mail (e-mail) facilities must not be used to:

- Access, view, download, print disseminate or post any material that may be considered inappropriate, offensive, defamatory, obscene, pornographic or discriminatory.
- Attempt to probe security mechanisms at the College or any other Internet sites.
- Post any information on Internet news groups, bulletin boards or similar forums on behalf of the College unless specifically authorised to do so.

During the course of network Internet session, students must not:

- Download any program.
- Play online games.
- Access any streaming media.
- Knowingly download a virus or similar program that will cause damage to the computer network.

### Removable media

The College understands that removable media is necessary for use with computer data transfer and storage. Because they are attached to the computer network the following rules apply

Users must:

- Ensure that all files are free of viruses.
- Accept responsibility for the maintenance of the device.

Users must not:

- Use the device for the storage of material that is prohibited by the network policy.
- Use the device for accessing prohibited material.

## Breach of Acceptable Use Policy and Consequences

Sanctions apply for breaches of the ICT Policy. The minimum penalty includes a 2 week ban and disciplinary action as determined by the Deputy Principal – Head of Campus.

### Student Acknowledgement form

I \_\_\_\_\_ have read the ICT Policy Guidelines and accept that the use of the Network is a privilege and that inappropriate use can lead to denial of access.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

### Parent Acknowledgement form

As the parent of \_\_\_\_\_ I \_\_\_\_\_ have read the ICT Policy Guidelines and accept that the use of the Network is a privilege and that inappropriate use can lead to denial of access to my child.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_