Information Communication & Technology (ICT) Acceptable Use Policy

Culture Statement:
St Mary's College, a Catholic educational community in the Christian Brothers tradition, is dedicated to the education and pastoral care of young men.
Through effective teaching, learning and values we aim to empower young men for:

- participation and leadership in all facets of today's and tomorrow's world;
- the development of a personal faith and spirituality.

Our challenge is to model relationships based on mutual respect; care for the individual; interdependence and collaboration; and service so that our students, growing in wisdom, justice and truth, will be enabled to contribute responsibly to their own transformation and that of society.
The values developed from our school Vision Statement and Mission Statement articulate what values underpin all aspects of life and learning at *St Mary's College*.

We Value *SUPPORT*….For each other in life long learning and faith

- Respecting each other and our environment
- Encouraging each other
- Acting with justice and integrity

We Value *STRIVING TOGETHER*.... in partnership with boys and their families

- Setting goals
- Working together
- Contributing to community development

We Value *SUCCESS*….In personal growth and learning

- Developing a strong work ethic
- Being optimistic
- Being the best person we can be

1. PREAMBLE
St Mary's College's computer and information network is a continually growing and changing resource that supports the users and systems. These resources are vital for the fulfilment of the academic and business needs of this community. In order to ensure a reasonable and dependable level of service, it is essential that each individual staff member, volunteer and student, exercise responsible and ethical behaviour when using these resources. Misuse by even a few individuals has the potential to disrupt the legitimate educational work of staff and students.
The provision of Information, Communication and Technology (ICT) systems by the College is to improve and enhance learning and teaching, and conduct of the business and functions of the College. Using information technology, accessing information, and communicating electronically can be cost-effective, timely and efficient. It is essential that use of this valuable resource be managed to ensure that it is used in an appropriate manner.
This policy outlines the application of the principles that govern our academic community in the appropriate use of College computer and information network resources. As it is impossible to anticipate all the ways in which individuals may misuse these resources, this policy focuses on a few general rules and the principles behind them.
This policy applies to the entire 'user' community (see 3.1 (viii) of the College and to the use of any and all College owned or managed computer-related equipment, computer systems, and interconnecting networks, as well as all information contained therein. It also covers the connection of personal / privately owned resources and their use within the College 'ICT systems'.)
The process by which the College seeks to manage use of the College ICT systems is through the development and implementation of this Policy. The Policy must be followed whenever using the College ICT systems.

2. Purpose

2.1 The purpose of this Policy is to ensure that all use of the *St Mary's College*; Toowoomba Information, Communications and Technology (***ICT***) systems is legal, ethical and consistent with the aims, values and objectives of the College as outlined in the College Vision and Mission Statements.

2.2 *St Mary's College*; Toowoomba's ICT systems must be properly and efficiently used. *St Mary's College*; Toowoomba' s ICT systems are not to be used for inappropriate activities including but not limited to pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment (including bullying and sexual), stalking, illegal activity and privacy violations.

3. Scope

3.1 In this Policy –

(i) an "Authorised Person" means the Principal or a person authorised by the Principal of *St Mary's College*, Toowoomba.

(ii) "copyright" does not include moral rights under the *Copyright Amendment (Moral Rights) Act 2000*

(iii) "College" means *St Mary's College*, Toowoomba;

(iv) "*St Mary's College*, Toowoomba ICT systems" includes, but is not limited to, College Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, Extranet, Internet, electronic mail (*email*), computer systems, software, servers, desktop computers, notebook computers, leased notebook computers, mobile phones, digital cameras, hand held and mobile devices (for example, personal digital assistants or "PDAs"), USB memory sticks and other ICT storage devices;

(v) "electronic communications" means Email, instant messaging and any other material sent electronically;

(iv) "personal use" means all non-work related use, and includes Internet usage and private emails.

(viii) "users" of the College ICT systems includes all employees (including ongoing, casual and temporary employees – both teaching and non-teaching staff) , students, volunteers, guests and contractors engaged by the College.

3.2 This Policy governs the use of the College ICT systems and includes but is not limited to:

- Publishing and browsing on the Internet (including Intranet and Extranet);
- Downloading or accessing files from the Internet or other electronic sources;
- Email;
- Electronic bulletins/notice boards;
- Electronic discussion/news groups;
- Weblogs ('blogs');
- File transfer, storage and sharing (including images, video and music);
- Video conferencing;
- Streaming media;
- Instant messaging;
- Online discussion groups and 'chat' facilities;
- Subscriptions to list servers, mailing lists or other like services;
- Copying, saving or distributing files;
- Viewing material electronically; and
- Printing material.

4.0 Use of Resources

All users are expected to utilise College resources in a responsible manner consistent with College policies and any guidelines and operating policies that the College (and its representative) may issue from time to time.

4.1 Acceptable Use

Acceptable uses of the network are activities which support teaching and learning. Network users are encouraged to use technology, computers and the Internet for purposes which meet their individual educational needs and take advantage of the computer and network functions;

Acceptable uses of technology, computers and the network include, but are not limited to

• network file storage
• the use of educational software applications
• electronic mail
• accessing databases
• accessing Internet resources

- creating content for use both 'off-line' and 'on-line'
- collaborating with other members of the College community and other on-line users.
- connection to and use of the College's learning management system.

4.2 Unauthorised Use

The unauthorised use of resources is prohibited and, in many cases, may be violations of the law. We are guided by the law in noting that unauthorised use includes, but is not limited to, the following types of activities.

4.2.1 Harassment or threats to specific individuals, or a class of individuals:

- Transmitting unsolicited information that contains obscene, indecent, lewd or lascivious material or other material which explicitly or implicitly refers to sexual conduct
- Using e-mail or newsgroups to threaten or stalk someone
- Transmitting unsolicited information that contains profane language or panders to bigotry, sexism, or other forms of prohibited discrimination
- Bullying and Harassment.

4.2.2 Interference or impairment to the activities of others:

- Creating, modifying, executing or retransmitting any computer program or instructions intended to:
  1. obscure the true identity of the sender of electronic mail or electronic messages, such as the forgery of electronic mail or the alteration of system or user data used to identify the sender of electronic e-mail
  2. bypass, subvert, or otherwise render ineffective the security or access control measures on any network or computer system without the permission of the owner; or
  3. examine or collect data from the network (e.g., a "network sniffer" program).
- Authorising another person or organisation to use your computer accounts or College network resources. You are responsible for all use of your accounts. You must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of your account by unauthorised persons. You must not share your password with anyone else or provide access to College network resources to unauthorised persons.
- Communicating or using any password, personal identification number, credit card number or other personal or financial information without the permission of its owner.

4.2.3. Unauthorised access and use of the resources of others:

- Use of College resources to gain unauthorised access to resources of this or other institutions, organisations, or individuals.
- Use of false or misleading information for the purpose of obtaining access to unauthorised resources.
- Accessing, altering, copying, moving, or removing information, proprietary software or other files (including programs, libraries, data and electronic mail) from any network system or files of other users without prior authorisation (e.g., use of a "network sniffer" program).
- Making unauthorised copies of copyrighted materials. You should assume all software, graphic images, music, and the like are copyrighted. Copying or downloading copyrighted materials without the authorisation of the copyright owner is against the law, and may result in civil and criminal penalties, including fines and imprisonment.
- Use of personal computers, laptops and other mobile resources, unless negotiated with the Authorised Person.
- Use of email and ICT to injure the reputation of *St Mary's College* or in a manner that may cause embarrassment to the College.

4.2.4. Unauthorised access and use of resources by others.

- Use of College resources by person/s not identified as a 'user' of the College ICT system, including technology supplied by the College to users for the expressed purpose of completing activities directly related to teaching and learning.
- Users (of the College ICT system) allowing non-users to access and use College ICT systems

4.3. Damage or impairment of College resources:

Use of any resource irresponsibly or in a manner that adversely affects the work of others. This includes intentionally, recklessly or negligently

1. damaging any system (e.g., by the introduction of any so-called "virus", "worm", or "trojan-horse" program or physical interference with a resource),
2. damaging or violating the privacy of information not belonging to you, or
3. misusing or allowing misuse of system resources.

Use of College resources for non-College related activities that unduly increase network load (e.g., chain mail, network games and spamming).

4.4. Unauthorised commercial activities:
Use of any College ICT resource

- for one's own commercial gain, or for other commercial purposes not officially approved by the College, including web ads.
- to operate or support a non-College related business.
- in a manner inconsistent with the College's contractual obligations to suppliers of those resources or with any published College policy.

4.5. Violation of state or federal laws:
Use of any College ICT resource that enables or assists the user in carrying out activities that breach state or federal laws including (but not limited to):

- Pirating software, music, videos and images
- Breach of copyright
- Discrimination and harassment
- Effecting or receiving unauthorized electronic transfer of funds
- Accessing and disseminating child pornography or other obscene material.
- Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.

4.6. When Inappropriate Use of Computer Resources Occurs
It is your responsibility to promptly report any violation of this policy or other College code, policy, guideline or agreement. In addition, you must report any information relating to a flaw in or bypass of resource security to the Principal or Authorised Person. Reports of unauthorised use or misuse of the resources will be investigated pursuant to standard College procedures. All illegal activities will be reported to local, state or federal authorities, as appropriate, for investigation and prosecution.
While the College desires to maintain user privacy and to avoid the unnecessary interruption of user activities, the College reserves the right to investigate unauthorised or improper use of College resources, which may include the inspection of data stored or transmitted on the network. In the event that use is determined to be contrary to College policy or applicable law, appropriate measures will be taken. These measures may include, but are not limited to, permanent or temporary suspension of user privileges, deletion of files, disconnection from the College network, referral to student or employee disciplinary processes and cooperating with the appropriate law enforcement officials and government agencies.
The College is not responsible for information, including photographic images and musical recordings, published on or accessible through personal web pages, including personal home pages. The College does not monitor the contents of these personal web pages. The individual or group creating or maintaining personal web pages is solely responsible for the content of the web page and may be held civilly and criminally liable for the materials posted on the web site.

5.0. Information on Applicable Laws and Statutes
All users of the College computer and information resources are expected to be familiar with and to abide by St Mary's College and Toowoomba Catholic Education Office codes and policies, as well as local, state and federal laws relating to electronic media, copyrights, privacy, and security.

6.0. Questions Relating to This Policy
The examples of unauthorised use set forth above are not meant to be exhaustive or exclusive. Additional questions about this policy or of the applicability of this policy to a particular situation should be referred to the College's Principal. The College Principal is the final authority on questions of appropriate use of College resources. If you are in doubt about whether any action could be deemed 'unacceptable', it is in the user's best interest to seek clarification before continuing to use College resources.

7.0. Responsibility
7.1 It is the responsibility of the Principal and anyone authorised by the Principal to ensure that the persons to whom this Policy applies are aware of this Policy. This may include, but is not limited to:
(a) providing access to a copy of the Policy on the College website;
(b) reminders of the need for compliance with the Policy; and

(c) providing updates or developments of the Policy, to those affected by the Policy.
7.2. It is the responsibility of all users to abide by the Policy.

8.0. Non-Compliance
8.1 Depending on the nature of the inappropriate use of the College ICT systems, non-compliance with this Policy may constitute:
(i) a breach of employment obligations;
(ii) serious misconduct;
(iii) sexual harassment;
(iv) unlawful discrimination;
(v) a criminal offence;
(vi) a threat to the security of the College's ICT systems;
(vii) an infringement of the privacy of staff and other persons; or
(viii) exposure to legal liability;
(ix) excessive personal use.
8.2. Non-compliance with this Policy will be regarded as a serious matter and appropriate action, including termination of employment or enrolment, may be taken.
8.3. Where there is a reasonable belief that illegal activity may have occurred the College will report the suspected illegal activity to the police.

9.0. Business Purposes
9.1 The College ICT systems are tools to be used for College purposes.
9.2 Use of College ICT systems must be for College purposes only, or where authorised or required by law, or with the express permission of an Authorised Person.
9.3 Notwithstanding clause 9.2, users of the College ICT systems may use the College ICT systems for personal use provided the use is not excessive and does not breach this Policy. Users must not engage in excessive personal use of the College ICT systems (including Internet and email). A breach of this clause constitutes non-compliance of this Policy.

10. Ownership
10.1 The College is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through the College ICT systems.
10.2 Electronic communications created, sent or received by the users referred to in clause 1.2 are the property of the College and may be accessed as records of evidence in the case of an investigation. Electronic communications may also be subject to discovery in litigation and criminal investigations. All information produced on computer, including emails, may be accessible under relevant FOI legislation.
Please note that email messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications have been held liable for messages that have been sent.
10.3 The College is the owner or asserts ownership and control over the physical resources of the network. This includes all computers, mobile devices and peripheral resources provided by the College for use by members of the College community. Users should not carry out any activity that causes disruption to the normal operation of individual resources or the network as a whole.

11. Monitoring
11.1 Use of College ICT systems will be monitored by Authorised Persons.
11.2 From time to time, Authorised Persons may examine or monitor the records of College ICT systems for purposes including, but not limited to, operational, maintenance, compliance, auditing, security or investigative reasons. For example, electronic communications and websites visited may be monitored. The College may investigate a complaint arising from the use of College ICT systems. Appropriate actions will be taken for users identified have breached appropriate use guidelines.
11.3 Use of the College ICT systems is provided to users on condition that it is agreed that College ICT systems are monitored in accordance with this Policy. Use of College ICT systems constitutes consent to monitoring in accordance with this Policy.
11.4 If at any time there is a reasonable belief that the College ICT systems are being used in breach of this Policy, the Principal or Authorised Person may suspend a users privilege of College ICT systems and may require that the equipment being used by the person be secured by the Principal or Authorised Person while the suspected breach is being investigated.
11.5 You should structure your email correspondence in recognition of the fact that *St Mary's College* may from time to time have the need to examine its content.

11.6 You should be aware that *St Mary's College* is able to monitor your use of the Internet, both during school or working hours and outside of these hours. This includes the sites and content that you visit and the length of time you spend using the Internet.

12. Defamation

12.1 College ICT systems must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or College liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

13. Copyright Infringement

13.1 The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or College liability, despite the belief that the use of such material was permitted.
13.2 *St Mary's College* supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.
13.3 All users of the College ICT systems should ensure they are familiar with publications relevant to the issue including (but not limited to)
(a) *Guidelines on Copyright and Trademark Management*; and
(b) *Copyright for Schools.*
and additional resources provided by Smartcopying (www.smartcopying.edu.au)

14. Illegal, Offensive or Inappropriate material

14.1 Use of the College ICT systems must be appropriate to a workplace environment. This includes but is not limited to the content of all electronic communications, whether sent internally or externally, intentionally or unintentionally.
14.2 The College ICT systems must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually oriented messages or images and messages that could constitute sexual harassment.
14.3 All users of the College ICT systems should be aware of their responsibilities under the Anti-discrimination Act 1991 (Qld), as well as *St Mary's College* harassment and bullying policies.
14.4 Students using the College ICT systems who receive unsolicited offensive or inappropriate material electronically should notify their teacher, Head of House, Head of Department E-Technology or Principal. Offensive or inappropriate material received from people known to the receiver should be deleted and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto the College ICT system except where the material is required for the purposes of investigating a breach of this policy.
14.5 Staff members using the College ICT systems who receive unsolicited offensive or inappropriate material electronically should delete, should not forward on and if concerned report to the Principal as soon as possible.
14.6 The College ICT systems must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority and their employment or enrolment at the College may be terminated.
14.8 Comments that are not appropriate in the workplace or school environment will also be inappropriate when sent by email. Email messages can easily be misconstrued. Accordingly, words and attached documents should be carefully chosen and expressed in a clear, professional manner.

15. Confidentiality

15.1 Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of the College ICT systems, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

16. Viruses

16.1 Viruses have the potential to seriously damage College ICT systems. Do not open any downloaded files, emails or attachments that you are not expecting or that look suspicious. In the event that a student receives any files that they suspect contain a virus it should be reported immediately to their supervising teacher. Staff members who receive any files that they suspect contain a virus it should be reported immediately to College Technicians.

17. Attribution

17.1 There is always a risk of false attribution of breaches of this Policy. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. If a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic communication has been intercepted or modified, the Principal or Authorised person should be informed.

17.2 Users are accountable for all use of the College's ICT systems that have been made available to them or loaned to them for work purposes and all use of the College's ICT systems performed with their individual user-ID. Users must maintain full supervision and physical control of the College's ICT equipment, including notebook computers and mobile devices, at all times. User-IDs and passwords must be kept secure and confidential. User-IDs and passwords should not be disclosed to anyone. Users must not allow or facilitate unauthorised access to the College's ICT systems through the disclosure or sharing of passwords or other information designed for security purposes.

18. Mass distribution and 'Spam'

18.1 The use of electronic communications for sending 'junk mail', for profit messages, or chain letters is strictly prohibited.

18.2 Mass electronic communications should only be sent in accordance with normal College procedures.

18.3 The use of electronic communications for sending unsolicited commercial electronic messages ('Spam') is strictly prohibited and may constitute a breach of the Spam Act 2003 (Cth).

19. Records Management

19.1 Electronic Communications are public records and subject to the provisions of the Public Records Act 2002 (Cth).

19.2 The College's record management practices for management of Email messages must comply with the College's policies and guidelines on recordkeeping and management of electronic communications as amended from time to time.

19.3 Email messages that are routine or of a short term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records.

19.4 Retention of messages fills up large amounts of storage space on the network and can slow down performance. As few messages as possible should be maintained in a user's mail box. Messages for archive should be kept in separate archive files stored on the user's network home or shared drive.

19.5 Email correspondence should be treated in the same way as any other correspondence, such as a letter or fax. That is, as a permanent written record which may be read by persons other than the addressee and which could result in personal or the College and by extension the Toowoomba Catholic Education Office liability.

19.6 You are/or the College may be liable for what you say in an email message. Email is neither private nor secret. It may be easily copied, forwarded, saved, intercepted, archived and may be subject to discovery in litigation. The audience of an inappropriate comment in an email may be unexpected and extremely widespread.

20. Disclaimer

20.1. All emails sent externally from the College's 'Web Email' service will automatically have a disclaimer attached to them. The current disclaimer is worded as follows:

Attention: This message is for the named person's use only. It may contain confidential, proprietary or legally privileged information. No confidentiality or privilege is waived or lost by any miss-transmission. If you receive this message in error, please immediately delete it and all copies of it from your system, destroy any hard copies of it and notify the sender. You must not, directly or indirectly, use, disclose, distribute, print, or copy any part of this message if you are not the intended recipient. *St Mary's College*, Toowoomba reserves the right to monitor all e-mail communications through its networks.

20.2. This disclaimer must not be altered or interfered with in any way, except by an Authorised Person. The use of this disclaimer may not necessarily prevent the College or the sender of the email from being held liable for its contents.

20.3 The College's 'Web Email' systems must also append the same disclaimer (above) to messages sent externally from the College's Email service.

21 Personal Use:
21.1 You are permitted to use the Internet and email facilities to send and receive personal messages, provided that such use is kept to a minimum and does not interfere with performance of your work/school duties.
21.2 However, you should bear in mind that any use of the Internet or email for personal purposes is still subject to the same terms and conditions as otherwise described in this Policy.
21.3 In the case of shared IT facilities, you are expected to respect the needs of your colleagues and use the Internet and email in a timely and efficient manner.
21.4 Excessive or inappropriate use of email facilities for personal reasons during working hours my lead to disciplinary action.

22. Privacy
22.1 In the course of carrying out your duties on behalf of *St Mary's College*, you may have access to, or handle personal information relating to others, including students, colleagues, contractors, parents and suppliers. Email should not be used to disclose personal information of another expect with the Toowoomba Catholic Education Office Privacy Guideline or with proper authorisation.
22.2 You should either lock your screen or log-out when you leave your desk. This will avoid other gaining unauthorised access to your personal information, the personal information of others and confidential information with *St Mary's College*.
22.3 In addition to the above, you should familiarise yourself with the National Privacy Principles ('NPPs') and ensure that your use of email does not breach the Privacy Act or the NPPs.

23. Complaints
23.1 If you wish to raise an issue about any activity relevant to this policy, see the College Principal.

24. Breaches of this Policy
24.1 Breaches of this Policy may be categorised using the following categories. The categories do not cover all breaches of this Policy, for example the categories do not specifically refer to breaches of copyright. Matters not covered by the following categories will be dealt with on an individual basis and on the relevant facts.
Category 1: Illegal
This category covers the following:
a. Child pornography – offences relating to child pornography are covered by relevant Acts.
b. Objectionable material – offences relating to the exhibition, sale and other illegal acts relating to "objectionable films" and "objectionable publications" are covered by relevant Acts
c. Any other material or activity which involves or is in furtherance of a breach of the criminal law.
Category 2: Extreme
This category involves non-criminal use of material that has or would attract a classification of **RC** under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth).
This covers any material that:
a) depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified;
b) describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not); or
c) promotes, incites or instructs in matters of crime or violence.
Category 3: Critical
This category involves other types of offensive material. This covers any material that:
a. contains depictions of actual sexual intercourse and other sexual activity between consenting adults;
b. involves racial or religious vilification;
c. is unlawfully discriminatory;
d. is defamatory;
e. involves sexual harassment; or
f. brings or has the potential to bring the employee and/or the College into disrepute.

25. Replacing previous policies

25.1 This Policy replaces any pre-existing College Acceptable Use Policies

25.2 This Policy is supported by, but does not replace the policies/agreements issued to students and parents titled:

St Mary's College – Student Acceptable Use of ICT Agreement

St Mary's College – Student Personal Laptop Use Agreement (special-needs).

25.3 This Policy is supported by, but does not replace the policies/agreements issued to staff titled:

St Mary's College – Staff Acceptable Use of ICT Agreement

St Mary's College – Staff Laptop Use Agreement

26. Accompanying Documents

26.1 This document should be read in conjunction with the following College documents

- Toowoomba Catholic Education - Code of Conduct
- *St Mary's College* – Student Acceptable Use of ICT Resources and Cybersafety
- *St Mary's College* – Conditions of Use of ICT Resources
- *St Mary's College* – Student Acceptable Use of Email Agreement
- *St Mary's College* – Student and Parent ICT Device Code of Conduct & Agreement
- *St Mary's College* – ICT Resources Access Consent Form.
- *St Mary's College* – Anti-Bullying Policy
- *St Mary's College* – Staff Laptop Use Agreement
- *St Mary's College* – Staff Acceptable Use of ICT Agreement – Cyber Safety
- *St Mary's College* – Cybersafety User Agreement
- *St Mary's College* – Parent & Student Handbook – 1 to 1 iPad Program