

ST JAMES' CATHOLIC SCHOOL BOARD OF TRUSTEES

CYBERSAFETY AND INTERNET USE POLICY

September 2010

Important terms used in this document:

- (a) *The abbreviation 'ICT' in this document refers to the term 'Information and Communication Technologies.*
- (b) *The term 'ICT devices' used in this document, includes but is not limited to, computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers (such as portable CD and DVD players), Gaming Consoles, and any other, similar, technologies as they come into use.*
- (c) *'School ICT' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (c) above*
- (d) *'Cyberspace' refers to the ICT devices as in (b) above, when connected to the global computer network (Internet) and its variety of digital information, including, but not limited to [World Wide Web](#), [electronic mail](#), [Voice over Internet Protocol](#) (VoIP), websites, blog sites, social networking sites and web feeds.*
- (e) *'Cybersafety' refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones*

RATIONALE

Nowadays, a large proportion of communication and flow of information occurs in "cyberspace". At St James' Catholic School, it is recognized that access to cyberspace by means of Information and Communication Technologies (ICT) is a tool for enhancing the teaching and learning occurring at school, as well as facilitating the effective operation of the school.

Thus, the Board of Trustees (BoT) at St James' Catholic School places a high priority on providing the school with Internet facilities and ICT devices. At the same time, the BoT at St James' Catholic School recognises that the presence of ICT in the learning environment can facilitate access to anti-social, inappropriate, and even illegal, material and activities. The BoT and teaching staff have the dual responsibility to maximize the benefits, and to minimise and manage the risks associated to the use of these technologies.

PURPOSE

The purpose of this policy is to provide the guidelines and procedures that, put in place, will result in rigorous and effective school cybersafety practices. In this way we endeavour to maximise the benefits of the use of Internet and ICT devices for teaching and student learning, for facilitating the effective operation of the school, while at the same time the risks associated to ICT use in our school are minimised and managed.

POLICY STATEMENT

St James' Catholic School will develop and maintain rigorous and effective cybersafety practices.

These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies.

GUIDELINES

To develop a cybersafe school environment, the board will delegate to the principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programmes. These will be based on the latest version of the NetSafe[®] programme for schools, endorsed by the New Zealand Ministry of Education. *The NetSafe[®] Kit for Schools*, including its templates for policies and use agreements, will play a central role in this process.

The Principal will report back to the BoT in the monthly Principals report under NAG3.

Cybersafety practices

1. The school's cybersafety practices are to be based on information contained in the latest version of the *NetSafe[®] Kit for Schools*, which is endorsed by the New Zealand Ministry of Education as best practice for New Zealand schools.
2. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.
3. St James' Catholic School use agreements will cover all board employees, all students, and any other authorised individuals to make use of the school Internet facilities and ICT devices/equipment. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
4. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
5. Use of the Internet and the ICT devices/equipment by staff, students and other approved users is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
6. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorised to make use of the Internet and ICT devices/equipment.
7. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times and from on-site or off-site locations.
8. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.
9. Issues relating to confidentiality, such as sighting student or staff information, reasons for collecting data and the secure storage of personal details and information (including images) will be subject to the provisions of the Privacy Act 1993.
10. The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. The response to individual incidents will follow the procedures developed as part of the school's cybersafety practices. In serious incidents, advice will be sought from an appropriate source, such NetSafe, the New Zealand School Trustees Association and/or a lawyer with specialist knowledge in this area. There will be special attention paid to the need for specific procedures regarding the gathering of evidence in potentially serious cases. If

illegal material or activities are suspected, the matter may need to be reported to the relevant law enforcement agency.

- Associated issues the school will address include:
- Funding for cybersafety practices ongoing through inclusion in the annual budget.
- The review of the school's annual and strategic plan.
- The deployment of staff, professional development and training.
- Implications for the design and delivery of the curriculum.
- The need for relevant education about cybersafety for the school community.
- Disciplinary responses appropriate to breaches of cybersafety.
- The availability of appropriate pastoral support, and potential employment issues.
- The need to protect the school computer network from unauthorized access.

DEFINITIONS

- ICT** Information and Communication Technologies.
- Authorised individuals** Such as teacher trainees, board members, external tutors and providers, contractors, and other special visitors to the school.
- 'Objectionable'** In this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.
- 'Cybersafety'** Refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones

RELATED DOCUMENTS

www.netsafe.org.nz/ua

APPENDIX

- Appendix One Staff Information and rules for use
- Appendix Two Staff Cybersafety Use Agreement
- Appendix Three Student information and rules for use
- Appendix Four Student Cybersafety Use Agreement

Signed:

Approval Date:

Review Team: D Pacheco, T. Edwards, C.Cogrove, L. Te Paiho

Next Review: September 2013

St James' Catholic School
Staff Information and rules for use

Instructions for staff

1. Please read the entire document carefully.
2. If any clarification is required, it should be discussed with the ICT Manager or the principal before the document is signed. Additional background information on use agreements can be found on the NetSafe website www.netsafe.org.nz/ua
3. Detach Appendix Two, sign and return it to the office.
4. It is important to retain the remaining pages for future reference.

Cybersafety Initiatives and Rules

The measures to ensure the cybersafety of St James' Catholic School (**herein referred as "the school"**) outlined in this document are based on our core values.

The school's computer network, Internet access facilities, computers and other school ICT devices bring great benefits to the teaching and learning programmes at St James' Catholic School, and to the effective operation of the school.

Our school has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

1. Cybersafety use agreements
 - 1.1 All staff, students and volunteers, *whether or not* they make use of the school's computer network, Internet access facilities, computers and other ICT equipment/devices in the school environment, will be issued with a use agreement.
 - 1.2 Staff are required to read these pages carefully, and return the signed use agreement form in Appendix Two to the school office for filing.
 - 1.3 The school's computer network, Internet access facilities, computers and other school ICT devices are for educational purposes appropriate to the school environment. Staff may also use school ICT for professional development and personal use which is both reasonable and appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on *or* off the school site.
 - 1.4 Any staff member who has a signed use agreement with the school and allows another person who does not have a signed use agreement to use the school ICT, is responsible for that use.
2. The use of any privately-owned/leased ICT equipment/devices on the school site, or at any school-related activity must be appropriate to the school environment. This includes any images or material present/stored on privately-owned/leased ICT equipment/devices brought onto the school site, or to any school-related activity. This also includes the use of mobile phones.
3. When using school ICT, or privately-owned ICT on the school site or at any school-related activity, users must not:
 - Initiate access to inappropriate or illegal material
 - Save or distribute such material by copying, storing, printing or showing to other people.
4. Users must not use any electronic communication (e.g. email, text) in a way that could cause offence to others or harass or harm them, put anyone at potential risk, or in any other way be inappropriate to the school environment.
5. Staff are reminded to be aware of professional and ethical obligations when communicating via ICT with students outside school hours.
6. Users must not attempt to download, install or connect any software or hardware onto school ICT equipment, or utilise such software/hardware, unless authorised by the ICT Manager.

7. All material submitted for publication on the school website/intranet(s) should be appropriate to the school environment. Such material can be posted only by those given the authority to do so by senior management.
8. All school ICT equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the ICT manager.
9. All users are expected to practice sensible use to limit wastage of computer resources or bandwidth. This includes avoiding unnecessary printing, unnecessary Internet access, uploads or downloads.
10. The users of school ICT equipment and devices must comply with the Copyright Act 1994 and any licensing agreements relating to original work. Users who infringe copyright may be personally liable under the provisions of the Copyright Act 1994.
11. Passwords must be strong, kept confidential and not shared with anyone else. A strong password is at least 8 characters in length with a mix of lower case (abd . . .) and upper case (ABC . . .) letters, symbols (#* @ . . .) and numerals (123 . . .).
12. Users (other than staff) should not allow any other person access to any equipment/device logged in under their own user account, unless with special permission from senior management.
13. The principles of confidentiality and privacy extend to accessing, inadvertently viewing or disclosing information about staff, or students and their families, stored on the school network or any ICT device. The Ministry of Education guidelines (www.tki.org.nz/r/governance/curriculum/copyguide_e.php) should be followed regarding issues of privacy, safety and copyright associated with student material which staff may wish to publish or post on the school website.
14. Dealing with incidents

14.1 Staff must follow procedures relating to the school cybersafety incident book.

14.2 Any incidents involving the unintentional or deliberate accessing of inappropriate material by staff or students, must be recorded in handwriting in the cybersafety incident book with the date, time and other relevant details.

In the event of access of such material, users should:

1. Not show others
2. Close or minimise the window, and
3. Report the incident as soon as practicable to the ICT Manager.

14.3 If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, it is necessary for the incident to be reported to ICT Manager IMMEDIATELY.

15. Any electronic data or files created or modified on behalf of St James' Catholic School on any ICT, regardless of who owns the ICT, are the property of St James' Catholic School.

16. Monitoring by the school

16.1 The school may monitor traffic and material sent and received using the school's ICT infrastructures.

16.2 The school reserves the right to deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email.

16.3 Users must not attempt to circumvent filtering or monitoring.

17. Breaches of the agreement

17.1 A breach of the use agreement may constitute a breach of discipline and may result in a finding of serious misconduct. A serious breach of discipline would include involvement with objectionable material, antisocial activities such as harassment or misuse of the school ICT in a manner that could be harmful to the safety of the school or call into question the user's suitability to be in a school environment.

17.2 If there is a suspected breach of the use agreement involving privately-owned ICT on the school site or at a school-related activity, the matter may be investigated by the school. The school may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

17.3 Involvement with material which is deemed 'objectionable' under the Films, Videos and Publications Classification Act 1993 is serious, and in addition to any inquiry undertaken by the school, the applicable

agency involved with investigating offences under the Act may be notified at the commencement, during or after the school's investigation.

18. The school reserves the right to conduct an internal audit of its computer network, Internet access facilities, computers and other school ICT equipment/devices, or commission an independent audit. If deemed necessary, this audit will include any stored content, and all aspects of its use, including email. An audit may include any laptops provided by or subsidised by/through the school or provided /subsidised by the Ministry of Education.

Please note that conducting an audit does not give any representative of St James' School the right to enter the home of school personnel, nor the right to seize or search any ICT equipment/devices belonging to that person, except to the extent permitted by law.

19. Queries or concerns

19.1 Staff should take any queries or concerns regarding technical matters to the ICT manager.

19.2 Queries or concerns regarding other cybersafety issues should be taken to the ICT Manager, or to the principal.

19.3 In the event of a serious incident which occurs when the ICT Manager and the principal are not available, another member of senior management should be informed immediately.

Staff requirements regarding students cybersafety

1. Staff have the professional responsibility to ensure the safety and wellbeing of children using the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices on the school site or at any school-related activity.
 2. If staff are aware that a student has not signed a use agreement, the student will not be permitted to use school ICT unless there are special circumstances approved by the principal.
 3. If staff are aware of any students who have not signed a use agreement their names should be reported to the principal, or to the ICT Manager.
 4. Staff should guide students in effective strategies for searching and using the Internet.
 5. While students are accessing the Internet in a classroom situation, the supervising staff member should be an active presence. The ICT Manager will advise about cybersafety protocols regarding Internet access by students in other situations.
 6. Staff should support students in following the student use agreement. This includes:
 - a. Endeavouring to check that all students in their care understand the requirements of the student agreement
 - b. Regularly reminding students of the contents of the use agreement they have signed, and encouraging them to make positive use of ICT.
 7. Staff are expected to follow the instructions of the ICT Manager regarding their role in maintaining cybersafety if students of the school are permitted email accounts. (Student email accounts may involve remote access, or access to private non-school email from within the school or on the school network).
-

St James' Catholic School
Staff Cybersafety Use Agreement

Please complete, sign, and date this Staff Use Agreement Form which confirms your agreement to follow the obligations and responsibilities outlined in this document. The key obligations and responsibilities are:

- All ICT use must be appropriate to the school environment
- Passwords will be kept confidential
- The principles of confidentiality, privacy and copyright apply.

If you have any queries about the agreement, you are encouraged to discuss them with the ICT Manager or the principal before you sign. Once signed, this form should be returned to St James' Catholic School (herein referred as "the school" office to be passed on to the ICT Manager for filing with staff records.

A copy of the signed form will be supplied to you.

This year the ICT Manager at St James' Catholic School is

Additional information can be found on the NetSafe website www.netsafe.org.nz/ua

Please tick one -	
<input type="checkbox"/>	I believe that I have sufficient knowledge to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/devices.
<input type="checkbox"/>	I require additional training/professional development in order to safely supervise the use made by students in my care of the school's computer network, Internet access facilities, computers and other school ICT equipment/ devices.

Use agreement

I have read and am aware of the obligations and responsibilities outlined in this Staff Cybersafety Use Agreement document, a copy of which I have been advised to retain for reference. These obligations and responsibilities relate to the cybersafety of students, the school community and the school environment.

I also understand that breaches of this Staff Cybersafety Use Agreement will be investigated and could result in disciplinary action, and where required, referral to law enforcement.

Name:

Role in the school:

Signature:

Date:

Instructions for parents*/caregivers/legal guardians

1. Please read the following sections carefully. If there are any points you would like to discuss with the school, let the school office know as soon as possible.
2. Discuss the cybersafety rules with your child.
3. Sign the Use Agreement Appendix Four and return that page to the school office.
4. Please keep the following sections for future reference.

*** The term ‘parent’ used throughout this document also refers to caregivers and legal guardians.**

Student Information and rules for use

The measures to ensure the cybersafety of St James’ Catholic School (herein referred as “the school”) outlined in this document are based on our core values.

The school’s computer network, Internet access facilities, computers and other school ICT equipment/devices bring great benefits to the teaching and learning programmes at Saint James’ Catholic School, and to the effective operation of the school.

Our school has rigorous cybersafety practices in place, which include cybersafety use agreements for all school staff and students.

The overall goal of the school in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school environment.

All students will be issued with a use agreement and once signed consent has been returned to school, students will be able to use the school ICT equipment/devices.

The school’s computer network, Internet access facilities, computers and other school ICT equipment/devices are for educational purposes appropriate to the school environment. This applies whether the ICT equipment is owned or leased either partially or wholly by the school, and used on *or* off the school site.

The school may monitor traffic and material sent and received using the school’s ICT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including email.

The school may audit its computer network, Internet access facilities, computers and other school ICT equipment/devices or commission an independent forensic audit.

These rules will help us to stay safe when using ICT at school

1. I cannot use school ICT equipment until my parent/s have signed my use agreement form (see Section C) and the completed form has been returned to school.
2. I can only use the computers and other ICT equipment for my schoolwork and only with my teacher’s permission.
3. I can only go online or use the Internet at school when a teacher gives permission and an adult is present.
4. If there is something I’m not sure about I will ask my teacher.
5. I will not use the Internet, email, mobile phones or any other ICT equipment to be mean, rude, or unkind about other people.
6. I will not tell anyone my password.

7. If I find anything that upsets me, is mean or rude, or things I know are not acceptable at our school, I will:

- Not show others
- Click on the '**Hector Safety Button**' or turn off the screen and
- Get a teacher straight away

8. I must not bring any ICT equipment/devices to school. This includes things like mobile phones, iPods, games, cameras, USB drives and software.

9. I will ask my teacher's permission before I put any personal information online.

Personal information includes:

- **Name**
- **Address**
- **Email address**
- **Phone numbers**
- **Photos.**

10. I will be careful and will look after all our school ICT equipment by:

- Not being silly and playing around with it
- Following our school cybersafety rules
- Telling a teacher about anything wrong or damaged.

11. I understand that if I break these rules the school may need to tell my parent(s).

St James' Catholic School
Student Cybersafety Use Agreement

To the parent/caregiver/legal guardian, please:

1. **Read this page carefully**, to check you understand your responsibilities under this agreement
2. **Sign the appropriate section on this form**
3. **Detach and return this form to the school office**
4. **Keep the document for future reference**, as well as the copy of this signed page which the school will provide.

I understand that St James' Catholic School (herein referred as "the school") will:

- Do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or school ICT equipment/devices at school, or at school related activities
- Work progressively with children and their families to encourage and develop an understanding of the importance of cybersafety through education designed to complement and support the use agreement initiative. This includes providing children with strategies to keep themselves safe in cyberspace
- Keep a copy of this signed use agreement on file
- Respond to any breaches in an appropriate manner
- Welcome enquiries from parents or students about cybersafety issues.

My responsibilities include:

- I will read this cybersafety use agreement document
- I will discuss the information with my child and explain why it is important
- I will return the signed agreement to the school
- I will support the school's cybersafety programme by encouraging my child to follow the cybersafety rules, and to always ask the teacher if they are unsure about any use of ICT
- I will contact the principal or school ICT Manager to discuss any questions I might have about cybersafety and/or this use agreement and I am welcome to do this at any time.

Additional information can be found on the NetSafe website www.netsafe.org.nz/ua

Please detach and return this section to school.

I have read this cybersafety use agreement and I am aware of the school's initiatives to maintain a cybersafe learning environment, including my child's responsibilities.

Name of student:

Name of parent/caregiver/legal guardian:
.....

Parent's signature: **Date:**

Please note: This agreement for your child will remain in force as long as he/she is enrolled at this school. If it becomes necessary to add/amend any information or rule, parents will be advised in writing.