

Cybersafety Policy

Important terms used in this document:

- (a) The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies.
- (b) '**Cyber safety**' refers to the safe and responsible use of the Internet and ICT equipment/devices, including mobile phones
- (c) '**School ICT**' refers to the school's computer network, Internet access facilities, computers, and other school ICT equipment/devices as outlined in (d) below
- (d) The term '**ICT equipment/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.

Rationale

Sacred Heart College has a statutory obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community. In addition Sacred Heart College Board of Trustees has a responsibility to be a good employer.

These three responsibilities are increasingly being linked to the use of the Internet and Information Communication Technologies (ICT), and a number of related cybersafety issues. The Internet and ICT devices/equipment bring great benefits to the teaching and learning programmes, and to the effective operation of the school.

The Board places a high priority on providing the school with Internet facilities and ICT devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

However, the Board recognises that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximise the benefits of these technologies, while at the same time to minimise and manage the risks.

The Board acknowledges the need to have in place rigorous and effective school cybersafety practices which are directed and guided by this cybersafety policy.

Policy

Sacred Heart College will develop and maintain rigorous and effective cybersafety practices which aim to maximise the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimising and managing any risks.

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.

Policy Guidelines

Associated issues the school will address include: the need for on-going funding for cyber safety practices 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 response appropriate to breach of cybersafety, the availability of appropriate pastoral support, and potential employment issues.

To develop a cybersafe school environment, the board delegates 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 regularly to the Board on issues relating to cybersafety.

Guidelines for Sacred Heart College 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 user agreement has been signed and returned to the school. User 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. Sacred Heart College user agreements will cover all board employees, all students (including adult and community), and any other individuals authorised to make use of the school Internet facilities and ICT devices/equipment, such as teacher trainees, external tutors and providers, contractors, and other special visitors to the school.
4. Use of the internet and the ICT devices/equipment by staff, students and other approved users at Sacred Heart College is to be limited to educational, professional development and personal usage appropriate in the school environment, as defined in individual user agreements.
5. Signed user 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.
6. Users, both students and adults, will be required to reconfirm their having read and understood the Sacred Heart College cybersafety policy and accept the terms of the user agreement annually at the beginning of each calendar year before access to technologies is enabled. This will be done by way of a confirmation box on the school intranet.
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.
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 students and staff 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.

Additional information can be found on the website
http://www.netsafe.org.nz/kits/kits_default.aspx