



# OUR HOLY REDEEMER

311 MONT ALBERT ROAD  
SURREY HILLS 3127

Telephone 9898 2315

Fax 9897 1137

Email [ohradmin@ohrsurreyhillscatholic.edu.au](mailto:ohradmin@ohrsurreyhillscatholic.edu.au)

Principal  
Frank Dame

Parish Priest  
Brendan Reed

## Cybersafety Policy

### **Important terms used in this document:**

- (a) The abbreviation '**ICT**' in this document refers to the term 'Information and Communication Technologies'.
- (b) '**Cybersafety**' 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), iPads, storage devices (such as USB and flash memory devices, CDs, DVDs, 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.

The world of digital learning beckons, with opportunities for teachers and students alike to benefit from the opportunities and capabilities a digital world offers. This policy, therefore, applies to all digital learning that takes place both at school and beyond the walls of the classroom.

### **RATIONALE**

Technological change in education means we are facing the largest transformation in how our students receive, interact with and respond to the learning experience that the teaching profession has ever seen. These changes mean that schools and early childhood settings are now broader than the walls of a classroom. Teachers, students and parents are increasingly using digital technologies to teach, learn and communicate, challenging the traditional concept of a school.

*'Creating and maintaining respectful, safe, secure and stimulating learning environments is an essential characteristic of a school that is engaging and inclusive of a diverse range of learners.'*

*A school also has a Duty of Care responsibility to identify known and foreseeable risks to students and to take reasonable steps to minimise these risks and to support students in their care. This includes*

*online and digital environments, particularly those that are created and/or owned by the school and its teaching staff.'*

*Teaching Safely in Online Spaces, DEECD*

## **AIMS**

This Cybersafety Policy has been developed to support students develop the skills needed for:

- critical evaluation;
- online collaboration and communication;
- behaviours which support the safe, responsible and ethical use of digital technology, which are essential to participating in life and work in the 21st century.

## **IMPLEMENTATION**

Staff are encouraged to implement the following guidelines when using digital technologies and social media tools with their students:

- Have a specific and clearly articulated educational purpose for using the technology and/or social media tool (group interchange, collaboration, etc.).
- Where possible, work with tools that are specifically designed for education.
- Be the administrator for every social media tool that is created for their students' use. This will allow teachers to moderate and edit content instantly.  
For more information, see: [Duty of Care in Online Spaces](#)
- Refer to each website or social media tool's specific terms and conditions. These will assist to determine whether the tool is appropriate for students or not (in particular, it is important to understand the requirements around privacy, safety, registrations, account security and protection of rights).  
For more information, see: [Things to Consider when Setting up a Social Media Profile](#)
- Obtain parent permission for students to register to use social media. Use this as an opportunity to inform parents / guardians about the social media tool you intend to use and its educational purpose.  
Obtain parent permission to publish student work and/or photos on the internet.  
For more information, see: [Consent Forms and Templates](#)
- Never publish personal information such as full names or addresses on the internet.  
Students should upload an avatar not a photo of themselves (For example, a 'voki' image, or DoppelMe avatar).
- Develop, in consultation with students and parents, agreements for the acceptable use of digital technologies and consequences of students behaving inappropriately online.
- Explicitly teach students the skills and knowledge to act safely and responsibly in the online world. Skills should be reinforced as new technologies are introduced.
- Encourage the school community to be supportive of the task by sharing the students' work with the wider school and community (e.g. via the school website, staff meetings, newsletters).
- Provide students with the [student technology audit](#). This can help teachers to establish how their students use technology and they can target their cybersafety lessons appropriately. Identifying the types and level of technology use within individual classes is also a useful conversation starter for identifying and addressing cybersafety issues.
- Ensure that student's do not include personal information (e.g. full name) as part of their email address. An email address such as [phi001@ohrsurreyhills.catholic.edu.au](mailto:phi001@ohrsurreyhills.catholic.edu.au) does not identify the student beyond the school. It would however allow the school to track the email and activities of that student.

### **Guidelines for Students**

1. No student may use the school Internet facilities and school-owned ICT devices/equipment in any circumstances unless Our Holy Redeemer School CyberSafety Practices are followed.
2. Use of the Internet and the ICT equipment by staff, students and other approved users at Our Holy Redeemer is to be limited to appropriate use in line with the statement, "Personal use of telecommunication resources is permitted provided it is limited to educational usage appropriate in the school environment, as defined in individual use agreements."
3. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools ICT devices/equipment and network facilities.
4. The safety of children is of paramount concern. Any apparent breach of CyberSafety Practices will be taken seriously and parents will be informed.

### **CYBERSAFETY PRACTICES**

- Students will not use school ICT equipment unless they are familiar with Our Holy Redeemer School CyberSafety Practices.
- Students will only use the computers and other ICT equipment with teacher permission and under adult supervision.

<b>Do Your Best</b> <ul style="list-style-type: none"><li>▪ Students will use the Internet for educational purposes only.</li><li>▪ If unsure of their online safety students will ask an adult for assistance.</li></ul>	<b>Be an Active Citizen</b> <ul style="list-style-type: none"><li>▪ Students must not deliberately access material of an inappropriate nature on the Internet.</li><li>▪ If a student inadvertently accesses anything inappropriate they will:<ul style="list-style-type: none"><li>- Turn the screen off</li><li>- Get a teacher straight away</li><li>- Not show others</li></ul></li></ul>
<b>Respect Others</b> <ul style="list-style-type: none"><li>▪ Students will not use the Internet, email, mobile phones or any other ICT equipment to be mean, rude, or unkind about other people.</li></ul>	<b>Respect Yourself</b> <ul style="list-style-type: none"><li>▪ Students will never enter any personal information about themselves (or others) on the Internet</li></ul>

- 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.
- Our Holy Redeemer's user agreements will cover all employees, all students, 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.
- The user agreements are also an educative tool.
- Use of the Internet and the ICT devices/equipment by staff and other approved users at Our Holy Redeemer is to be limited to educational, professional development, and personal usage appropriate in the school environment, provided it is not for commercial gain or in any way counter productive to the business and reputation of Our Holy Redeemer School.

- 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.
- 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.
- The school has the right to audit at anytime any material or 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.
- 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 as the ACMA (Australian Communications and Media Authority), the CEM (Catholic Education Melbourne) 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.

### **ONLINE ETIQUETTE OF PARENTS, CARERS & SCHOOL STAFF**

Parents, carers and staff are expected to adhere to high standards of online etiquette when using online communications within the school community in order to model safe and responsible use of social media and digital technologies. Only then will our children be able to make informed, respectful decisions about what they share online.

### **REVIEW**

- The Parish Education Board and staff regularly monitor and review the effectiveness of the Cybersafety policy (at least once every three years) and revise the policy when required.

This policy was last endorsed by the Parish Education Board on...

November 2018

### **Relevant Documents / Links**

Australian Communications and Media Authority CyberSmart Schools Gateway

The Grid – New Zealand

DEECD Learning Online

ACMA CyberSmart Connect.ed

<http://www/digizen.org/>