

OLSH College Cyber Safety Policy

Preamble

Our Lady of the Sacred Heart College (**OLSH College**) is committed to providing a safe and secure learning environment for students and to developing students as responsible cyber citizens who demonstrate ethical behaviour when using online and digital technologies.

Whilst valuing digital technologies as a learning tool, the College remains vigilant in maintaining safe, inclusive and respectful online learning environments. We endeavour to reduce students' exposure to cyber risks, which can include, but are not limited to, online grooming, cyberbullying, trolling, scams, image-based abuse, harmful or unlawful online conduct, unauthorised access to accounts or systems, misuse of artificial intelligence or synthetic media, and access to inappropriate content.

A whole-school approach is used to develop a culture of safety and to prevent risks to online safety. We recognise that our learning environments extend beyond the school grounds and include online and virtual College Environments and we endeavour to work in partnership with parents guardians and carers to raise awareness of cyber safety in settings beyond the school.

Purpose

This policy sets out the way in which cyber safety is enhanced at OLSH College and risks to student safety and wellbeing are addressed. It also records the College's statement on online conduct and online safety for the purposes of *Child Safe Standard 9 and Ministerial Order No. 1359*, without duplicating the College's broader Child Safety and Wellbeing Policy.

It complements a range of College policies for acceptable use of digital technologies (refer to *References and Legislative Context* section below), in particular:

- OLSH College Student Electronic Resources Policy
- OLSH College Laptop Conditions of Use Policy
- OLSH College Mobile Phone and Digital Technology Policy
- OLSH College Child Safety and Wellbeing Policy
- OLSH College Respectful Relationships Policy
- OLSH College Bullying Prevention Policy

Scope

This policy applies to all students, staff and other members of the College Community when they use, access, supervise, administer or support digital technologies or online environments connected with the College. It applies in College Environments, including on College premises, online and virtual environments made available or authorised by the College, College Activities, and other locations or online services provided by the College or through third-party providers for student use.

Conduct occurring outside College Environments may be addressed under this policy where it has a sufficient connection to the College, student safety or wellbeing, the College's reputation, or the rights and safety of members of the College Community

Principles

- Every student has a right to be safe in both physical and online environments.
- Students are encouraged and supported to raise cyber safety concerns, contribute to discussions about online safety and participate in creating safe and respectful online environments.
- The use of digital technologies in our learning environments facilitates the development of valuable skills and knowledge and prepares students to thrive in our globalised and inter-connected world.
- Digital technologies, if not used appropriately, present risks to students' safety and wellbeing. The College is committed to educating students to use digital technologies safely, ethically and responsibly in the school environment and in off-campus settings.
- Staff have a duty of care to take reasonable steps to protect students from any harm that should have reasonably been foreseen, including those that may be encountered within off-campus online learning environments.
- A whole-school approach is adopted to address cyber safety. This includes working in partnership with families to reduce or remove the risks to the personal safety and wellbeing of our students.
- Compliance with accompanying school policies and practices pertaining to child safety and Victoria's Child Safe Standards under Ministerial Order No. 1359 is essential in supporting a culture of online safety for students.
- The College will seek to identify and mitigate risks in online environments in a way that promotes child safety and wellbeing while respecting students' privacy, access to information, social connections and learning opportunities.
- Online incidents will be responded to promptly, proportionately and in accordance with the relevant College policy or reporting pathway, including child safety, anti-bullying, privacy, complaints, student behaviour and staff conduct processes as applicable.

Procedures

Cyber Safety Education

Cyber safety education and cyberbullying prevention strategies are implemented across year levels on a continuous basis, with a focus on teaching age-appropriate content, skills and strategies to empower students to recognise cyber safety issues and respond appropriately.

Online safety risks addressed include:

- Cyberbullying and trolling
- invasion of privacy or digital surveillance
- inappropriate sharing of images
- phishing, harvesting of personal information or data theft
- identity theft
- malicious software (malware)
- offensive images and messages
- impersonation/catfishing
- grooming
- unsafe or inappropriate use of age-restricted social media platforms
- misuse of generative artificial intelligence, synthetic media or deepfakes
- unsafe external access or communication with people outside the College in online environments.

We also educate our students about digital issues such as privacy, intellectual property and copyright, and the importance of maintaining their own privacy and security online, including protecting their passwords. Students are aware that they must immediately notify their Learning Mentor or House Leader if they know or suspect their account has been used by another person.

Student Behavioural Expectations

Safe use of digital technologies is underpinned by the behaviours described in the College's *Respectful Relationships Policy*. It is also guided by the College's *Electronic Facilities and Resources Policy*.

Students are responsible for their behaviour when using the College's network and digital resources. They must comply with the College's expectations and honour the College's *Student Electronic Resources Policy*.

The College has clear protocols in place for students' acceptable use of their devices while on campus. These are outlined in our *Mobile Phone and Digital Technology Policy*.

The College's *Bullying Prevention Policy*, incorporating cyberbullying, encourages a culture that is firm about the unacceptable nature of bullying. It articulates how bullying and cyberbullying are defined and addressed, including the means taken to prevent incidents and the response

taken when bullying or cyberbullying occurs. Reporting cyber safety incidents is encouraged, taken seriously and promptly addressed, with response strategies tailored to the circumstances of each incident.

Behavioural issues involving cyberbullying, discrimination or harassment will be managed under this policy together with the College's Respectful Relationships Policy and Bullying Prevention Policy, as applicable.

Breaches of any of the above-mentioned policies by students may result in a number of consequences, which will depend on the severity of the breach and the context of the situation, and will be managed consistently with procedural fairness, student wellbeing considerations and any applicable child safety obligations.

Reporting and responding to cyber safety incidents

Students, parents, guardians, carers and staff are encouraged to report cyber safety concerns as soon as practicable. Students may report concerns to their Learning Mentor, House Leader, the Deputy Principal Student Wellbeing, or any other trusted staff member.

Parents, guardians and carers may report concerns through the Principal, member of the College Leadership Team or the College's Complaints Resolution Policy process.

Where a cyber safety concern involves alleged child abuse, grooming, reportable conduct, a risk of significant harm, family violence or other conduct requiring external reporting, staff must follow the College's child safety and reporting policies, including the PROTECT Four Critical Actions and any mandatory reporting, reportable conduct, police reporting, information sharing and record keeping obligations. The College will document and retain records of reported cyber safety concerns and incidents in accordance with applicable child safety, privacy, information sharing and records management requirements.

Where there is an emergency or immediate risk of harm, emergency services should be contacted.

Parent/Family Partnerships

The College recognises that students are best taught in partnership between home and the College. Information is periodically provided to parents, guardians and carers, at parent information evenings and via our newsletter, about cyber safety risks and prevention and intervention strategies that may mitigate these risks.

Parents, guardians and carers are aware of the College's expectations of students for responsible, ethical and safe use of digital technologies. They are co-signatories to our *Student Electronic Resources Policy - Student Acceptance form*.

Responsible reporting of inappropriate online behaviour is encouraged when parents, guardians and carers observe such behaviour either being perpetrated by, or targeted at, a student. Cyber safety concerns and complaints, when reported to the College, are addressed in a timely manner, with the responses tailored to the circumstances of each incident.

College Safeguards

The College's practice in the use of digital technologies is informed by the Australian Government eSafety Commissioner. Staff endeavour to keep up to date with current online safety issues and seek expert advice from this authority.

Staff supervise and support students using digital technologies for their schoolwork, including where programs are delivered virtually via video conferencing platforms, off-site, or by another school or instructor while our students remain onsite, and when students are engaged in digital learning in the classroom or other College Environments.

The College provides a filtered internet service to block access to inappropriate content. The College acknowledges that filtering is an important safeguard but cannot guarantee full protection from all inappropriate or harmful content. Staff also review the safety and appropriateness of online resources and remove offensive content at the earliest opportunity. Breach reports are logged and checked on a regular basis.

Before adopting digital technologies, software, applications, online services or third-party platforms for student use, the College will consider whether they have an appropriate educational or administrative purpose and whether privacy, cybersecurity and child safety risks have been assessed and mitigated.

The College will not require or direct students to create accounts on age-restricted social media platforms for learning activities. Where content from an age-restricted platform has a genuine curriculum-aligned purpose, it should be accessed in a manner that does not require students to create or use an account, unless permitted by law, platform terms and College policy.

Staff and students are aware that all messages and files created, sent, stored or retrieved on the College network are the property of OLSH College, and that the College reserves the right to access and monitor all messages and files as necessary and appropriate in accordance with law, the College's *Privacy Policy*, applicable notices and College policies.

Definitions

Where the following terms are used in this policy, they have the meaning set out below.

Acceptable Use Agreement means an agreement, acknowledgement or set of expectations issued by the College for student, staff or other user access to College digital technologies, systems, networks or online services.

Child abuse includes any act committed against a child or young person involving:

- a sexual offence
- grooming
- physical violence
- serious emotional or psychological harm
- serious neglect.

Child safety encompasses matters related to protecting all children from abuse, managing the risk of abuse, providing support to a child at risk of abuse, and responding to incidents or allegations of abuse.

College or OLSH College means Our Lady of the Sacred Heart College Bentleigh.

College Activities means any activity, event or program organised, authorised or facilitated by the College, whether conducted on College premises, online or at another location, including camps, excursions, sporting events, performances, retreats and co-curricular activities.

College Community means students, staff, parents, carers, guardians, volunteers, contractors, visitors and other persons participating in College Activities or using College Environments.

College Environments means physical, online and off-site environments provided, authorised or managed by the College, including College Activities and digital platforms, online services and social media connected with College Activities.

Cyber abuse means behaviour that uses technology to threaten, intimidate, harass or humiliate someone — with the intent to hurt them socially, psychologically or even physically. Cyber abuse can take place on social media, through online chat and messaging services, text messages, emails, on message boards and in online forums that allow people to comment publicly.

Cyberbullying means the use of technology to bully someone — to deliberately and repeatedly engage in hostile behaviour to hurt them socially, psychologically or even physically. It is generally used to refer to the online abuse of children and young people. Groups and individuals can be both the perpetrators and targets of cyberbullying. Cyberbullying can take

place on social media, through online chat and messaging services, text messages, emails, on message boards and in online forums that allow people to comment publicly.

Cyber safety refers to the safe and responsible use of digital technologies. This includes privacy and information protection, respectful communication, and knowing how to get help to deal with online issues.

Digital technologies means electronic tools, systems, devices and resources that generate, store or process data, including hardware, software, apps, websites, learning platforms, collaboration tools, email, messaging, video conferencing, artificial intelligence tools and online services.

External access means communication in an online environment with individuals or parties outside the College.

Family violence is defined under the *Family Violence Protection Act 2008* (Vic.) to include behaviour that causes a child to hear, witness or be exposed to the effects of family violence such as abusive, threatening, controlling or coercive behaviour. While family violence does not form part of the official definition of 'child abuse' in the *Child Wellbeing and Safety Act 2005* (Vic.), the impact of family violence on a child can be a form of child abuse, for example, where it causes serious emotional or psychological harm to a child. A child can also be a direct victim of family violence.

Grooming means when an adult deliberately establishes an emotional connection with a child in order to lower their inhibitions, and to make it easier to have sexual contact with them. It may include adults posing as children in chat rooms or on social media sites to 'befriend' a child in order to meet with them in person. Grooming can include obtaining intimate images of young people.

Inappropriate content means material that is illegal or developmentally inappropriate that is shared or accessed online. This can include posting of inappropriate images or comments. It can also include accessing online platforms that contain harmful material.

Image-based abuse is when intimate photos or videos are shared online without the consent of the person in the photo or video. Even threatening to share intimate images in this way is image-based abuse. It is a criminal offence under state and territory laws. Alternative terms for image-based abuse include 'non-consensual sharing of intimate images', 'revenge porn' or 'intimate image abuse'. Image-based abuse can also arise when a photo or video is digitally altered (for example, photoshopped), or when a person is depicted without religious or cultural attire which they would usually wear in public.

Mandatory report is a report made to Child Protection, by a person mandated under the *Children, Youth and Families Act* (2005), that is based on a reasonable belief that a child is in

need of protection from injury that results from abuse or neglect or harm caused as a result of abuse (emotional, physical or sexual) or neglect, including medical neglect.

Physical violence occurs when a child suffers or is likely to suffer significant harm from a non-accidental injury or injuries inflicted by another person. Physical violence can be inflicted in many ways including beating, shaking, burning or using weapons (such as belts and paddles). Physical harm may also be caused during student fights.

Reasonable belief is when a person is concerned about the safety and wellbeing of a child or young person, they must assess that concern to determine if a report should be made to the relevant agency. This process of considering all relevant information and observations is known as forming a 'reasonable belief'. A 'reasonable belief' or a 'belief on reasonable grounds' is not the same as having proof but is more than mere rumour or speculation. A 'reasonable belief' is formed if a reasonable person in the same position would have formed the belief on the same grounds.

Reportable conduct covers allegations or convictions of child abuse or misconduct toward children where the source of the misconduct or conviction is an employee of an organisation. It is defined under the *Child Wellbeing and Safety Act 2005* (Vic.) to mean a sexual offence, sexual misconduct or physical violence committed against, with or in the presence of a child, behaviour causing significant emotional or psychological harm to a child, or significant neglect of a child.

Scams are dishonest schemes that seek to take advantage of people to gain benefits such as money or access to personal details.

School environment is any physical or virtual place made available or authorised by the school for use by a child or young person during or outside school hours, including:

- a campus of the school
- online school environments
- locations used for school camps, sporting events, excursions, competitions, and other events.

Serious emotional or psychological harm. Serious emotional or psychological abuse may occur when a child is repeatedly rejected, isolated or frightened by threats or the witnessing of family violence. It also includes hostility, derogatory name-calling and put-downs, or persistent coldness from a person, to the extent where the behaviour of the child is disturbed or their emotional development is at serious risk of being impaired. Serious emotional or psychological harm could also result from conduct that exploits a child without necessarily being criminal, such as encouraging a child to engage in inappropriate or risky behaviours.

Serious neglect includes a failure to provide a child with an adequate standard of nutrition, medical care, clothing, shelter or supervision. Significant neglect causes harm to a child that is more than trivial or temporary. Serious neglect is when the child is exposed to an extremely

dangerous or life-threatening situation and there is a continued failure to provide a child with the basic necessities of life.

Student refers to a child or young person enrolled at OLSH College Bentleigh.

Trolling is when a user intentionally makes inflammatory comments in an online public forum in order to provoke anger or argument and disturb other users. Individuals who engage in trolling (called 'trolls') seek an emotional response from others, whether with malicious or humorous intent. Responding to trolling comments can result in an escalation of inappropriate communication.

References and Legislative Context

This policy is informed by the following guidance, laws and standards, as amended or replaced from time to time:

- Australian Government eSafety Commissioner resources, including the Toolkit for Schools and cyberbullying advice for educators and schools
- *Child Wellbeing and Safety Act 2005* (Vic), *Children, Youth and Families Act 2005* (Vic), *Crimes Act 1958* (Vic), *Privacy Act 1988* (Cth), *Health Records Act 2001* (Vic), *Worker Screening Act 2020* (Vic) and other applicable child safety, privacy, equal opportunity and occupational health and safety laws
- Department of Education , [*PROTECT: Identifying and responding to all forms of abuse in Victorian schools*](#)
- Department of Education, *PROTECT: Identifying and Responding to Student Sexual Offending*
- *Education and Training Reform Act 2006* (Vic) and *Education and Training Reform Regulations 2017* (Vic)
- Ministerial Order No. 1359 Implementing the *Child Safe Standards – Managing the Risk of Child Abuse in Schools and School Boarding Premises*,
- *Online Safety Act 2021* (Cth) and *Online Safety Amendment (Social Media Minimum Age) Act 2024* (Cth)
- Victorian Government, *PROTECT Four Critical Actions for Schools*

Related College Policies

- Child Safety Code of Conduct
- Child Safety Student Rights and Responsibilities Policy
- Child Protection Reporting Responsibilities Policy
- Complaints Resolution Policy
- Student Electronic Resources Policy
- Student Laptop Conditions of Use Policy
- Privacy Policy
- Respectful Relationships Policy
- Staff Responsible Use of Social Media policy and procedure
- Bullying Prevention Policy
- Mobile Phone and Digital Technology Policy

Policy History and Review

At OLSH College, we are committed to continuous improvement of our child safety systems and practices. We intend this policy to be a dynamic document that will be regularly reviewed to ensure it is working in practice and updated to accommodate changes in legislation or circumstance, regulatory guidance, College practice, technology, and emerging risks in physical and online environments.

Responsibility	OLSH College Principal and College Board Policy Committee
Reviewed and revised	August 2022, August 2026
Next Review Date	August 2028