De La Salle College

Cyber Safety Policy

De La Salle College is a school which operates with the consent of the Catholic Archbishop of Melbourne and is owned, operated and governed by Melbourne Archdiocese Catholic Schools Ltd (MACS).

When children/young people have access to internet-enabled devices, they also have access to an extensive amount of content across the internet, social media and other applications. As a College community, all staff and parents have a responsibility to enable students to maintain healthy, life-affirming relationships online and to use technology safely.

This Cyber Safety Policy aims to maximise the benefits of the Internet and Information, Communication and Learning Technologies, while at the same time minimising the dangers and managing the risks of cyber bullying within the College community.

Furthermore, it seeks to:

1 Develop and maintain effective cyber safety practices which maximise the beneficial use of information communication and learning technology (digital) for student learning;

2 Educate students, staff and parents on how to use digital platforms safely and responsibly as detailed in the Student Notebook Agreement available the College Learning Management System OLLIE;

3 Enable students to learn how to protect their own privacy and not infringe the rights of others in an online environment;

4 Establish practices to on how to respond to inappropriate use of digital platforms that infringes the rights of others.

Definitions

Ensuring cyber safety involves the active promotion of cyber safe behaviours based on the safe, respectful and responsible use of internet and mobile phone technologies, and the taking of specific measures to remove the risks of any inappropriate and harmful use of these technologies.

At De La Salle College, cyber bullying refers to the deliberate and repeated misuse of technology to harass, threaten, insult or ridicule students or staff. Examples include threatening texts, emails or direct messages, online denigration, vilification or defamation, derogatory websites, disturbing private pictures or videos, and online exclusion or impersonation. Victims of cyber bullying can include both students and staff.

Aggression: Angry or violent behaviour or feelings; or hostile action against another member of our College community or their family.

College Assets: The College's network, Internet access facilities, computers, and other College digital equipment/devices (as outlined below).

Cyber bullying: Includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening another person by sending or posting inappropriate and hurtful email messages, instant messages, videos, text messages, phone messages, digital pictures or images, or website postings (including blogs).

Cyber safety: The safe and responsible use of the Internet and digital equipment/devices, including mobile phones.

Digital Equipment and Devices: Includes but is not limited to; computers (such as desktops, notebooks, laptops, PDAs), storage devices and digital devices, cameras (such as video, digital, webcams), all types of mobile phones, video and audio players/receivers, gaming consoles, and any other, similar, technologies as they come into use.

Safe school: A safe school is one where the physical environment is safe and does not lead to harm or injury for students; the emotional environment is one of positivity and free from negative behaviours such as bullying which can affect mental health; and where a healthy lifestyle is promoted through initiatives such as increased participation in sport and/or healthy food at the canteen.

Student wellbeing: Wellbeing is the degree to which a student is functioning effectively in the school community. Student wellbeing refers to a sustainable state of positive mood and attitude, resilience and satisfaction with self, relationships and experiences at school.

Violence: The use of emotional or physical force to harm someone within our College community.

Student and Staff Responsibilities

The ever-changing nature of the internet poses some unique challenges and opportunities for our College community.

If any of the behaviours below occur either during College time or after College hours, it will constitute a breach of Cyber Safety Policy and as such a student will be subject to appropriate consequences as determined by College staff. Students must be aware that in certain circumstances where a crime has been committed, they may also be subjected to a criminal investigation by the police over which the College will have no control.

1. The College name, motto, crest, logo and/or uniform must not be used in any way which would result in a negative impact for the College and its community;
2. Students must not post any materials created at school, or as part of the College's program, without permission from the College;
3. Students must not post photos or videos of either themselves and/or other students or staff which denigrate, insult, humiliate or hurt those involved, or without their permission;
4. Members of the College community have a responsibility to ensure that all online communications are in keeping with the College's expectations in relation to appropriate and respectful interactions with teaching and non-teaching staff;
5. Members of the College community will not post inappropriate comments about individual staff members or students, which if said in person, would result in disciplinary action being taken;
6. Neither the College's network nor the broader internet (whether accessed on campus or off campus, either during or after College hours, via any application) may be used for any purpose other than that which it was designed;
7. Cyber bullying, harassment, taking, sending and receiving naked or sexually explicit images (sexting), and other misuses of technology in cyberspace are unacceptable.

Students and staff who feel that they have been the victims of such misuses of technology should save and store the offending material on their computer, mobile phone or other device. They should then print a copy of the material and immediately report the incident to a staff member. Staff who may have been cyber bullied or threatened online should immediately report such incidents to a member of the Executive Team. However, if the bullying material involves sexualised images, be aware that possessing or sharing such images of people under 18 may be a crime, even if you have just taken a screenshot for evidence purposes.

All reports of cyber bullying and other technology misuses will be investigated fully and may result in a notification to Police where the College is legally obliged to do so. Sanctions may include, but are not limited to, the loss of computer privileges, detention, suspension, or expulsion from the College.

Parent / Caregiver Responsibilities

Bullying is a serious issue for everyone. It can happen anywhere, anytime, and can have devastating consequences.

Parents / caregivers can help to reduce incidents of cyber bullying by:

- Establishing and maintaining trust and setting healthy limits for the amount of time spent online each day;
- Recognising that for many children/young people, their online life is an important part of their social identity;
- Monitoring home use by students and report to the College any communications that may have the effect of breaching this policy;
- Implementing boundaries such as only using devices in 'safe spaces', like the living room, or having an open-door policy when children/young people use devices or computers in the bedroom;
- Reporting the cyber bullying material to the social media service where it happened;
- Collecting details of the cyber bullying material by taking a photo or copying the URL;
- Reporting cyber bullying or illegal material to the Office of the Children's eSafety Commissioner, see: Office of the Children's eSafety Commissioner;
- Blocking or unfriending the person so they cannot continue to upset your child/young person while the content is being removed.

Monitoring by the College

1. The College reserves the right at any time to check work or data on the school's computer network, Internet access facilities, computers and other school digital equipment/devices without obtaining prior consent from the relevant Authorised User. For example, the College may at any time check student email or work;
2. The College reserves the right at any time to check work or data on College owned digital equipment on the school site or at any school-related activity;
3. The College has several electronic access monitoring systems which have the capability to record email and Internet use, including the user details, time, date, sites visited, length of time viewed, and from which computer or device;
4. The College monitors traffic and material sent and received using the College's digital infrastructures. From time to time this may be examined and analysed to help maintain a Cybersafe environment;
5. The College may deploy filtering and/or monitoring software where appropriate to restrict access to certain sites and data, including email;
6. The College will clearly indicate during the logon process that all members, by logging on, are bound by the College ICT policies;
7. The College may from time to time conduct an internal audit of its computer network, Internet access facilities, computers and other school digital equipment/devices, or may commission an independent audit of content and usage.

Related Policies

Student Bullying Prevention Policy
Staff Code of Conduct
Pastoral Care Policy
Privacy Policy
Student Code of Conduct
Complaints Handling Policy
Student Notebook Agreement
ICT Policy

Related Legislation

Building Safe and Respectful Schools (DET) 2016
Bully Stoppers (DET) 2016
Disability Discrimination Act 1992
Education Services for Overseas Students (ESOS) Act 2000
Human Rights and Equal Opportunity Commission (HREOC) Act 1986
Racial Discrimination Act 1975
Racial Hatred Act 1995
Sex Discrimination Act 1984

Approval

Responsible officer:	Deputy Principal - Students
Approval Body:	Executive Team
Approval Date:	17.08.2021
Amended:	15.12.2022
Previous approval:	November 2016
Next scheduled review:	August 2024