

Purpose

This policy seeks to ensure that measures are in place to create and maintain a culture of cybersafety that is in keeping with the Bayside Christian College (College) values, including the Bayside Way and its eSmart Values, and is consistent with legislative and professional obligations.

The College is committed to:

- promoting the appropriate use of ICT by all members of the College community that ensures the safety and wellbeing of all students, staff and parents/carers, emphasising zero tolerance to cyberbullying.
- ensuring students, staff and parents are aware of their roles and shared responsibilities in relation to cybersafety and appropriate online behaviours.
- developing the skills, knowledge, attitudes and behaviours required of students, staff and parents to participate and function responsibly, safely and appropriately in cyberspace.

Application

This policy applies to staff, contractors, volunteers, students and parents/carers of the College who use any computing, network, printing, internet, or other College ICT resource whilst at the College, from any external location, or at College endorsed activities.

Policy Statement

- The College focuses on continually improving its footprint in providing effective cybersafety practices in line with its values and eSmart Values.
- The College provides a range of opportunities to promote awareness and educate on cybersafety. This includes, but is not limited to:
 - Educating students by providing educational sessions on digital media literacy, understanding cyberbullying, positive online behaviour, peer and personal safety;
 - Educating parents/carers by providing parent information sessions, newsletter items outlining the College's cybersafety policy and procedures;
 - Educating contractors and volunteers via the online induction upon commencement of work for and at the College;
 - Educating staff by providing professional development training, webinars, and risk management practices.
- The College has an ICT User Agreement that parents and students agree to as a condition of entering the College which underpins the College values and mission statement. This covers obligations, responsibilities and possible consequences.

- The College allocates sufficient resources to continually review and mature an effective cybersafety culture. This includes cybersafety as a standard item on the Information and Communication Technology (ICT) Committee meeting agenda.
- The College uses a risk-based approach when engaging with any new products and services to ensure it has the highest safety, privacy and security standards as reasonably practicable.

Definitions

Cybersafety	The way in which users behave responsibly online to keep themselves and their friends safe. It incorporates the safe and desirable use of the internet and ICT equipment and devices, an awareness of our digital footprint, and how to behave appropriately and respectfully.
Cyberbullying	Direct verbal or indirect bullying behaviours using digital technologies. E.g., repeated inappropriate comments on social media spaces.
eSmart Values	The College's eSmart values show that we: "C.A.R.E"- Care for And Respect Everyone.
ICT Resources	Includes, but is not limited to, computers (e.g., servers, desktops, laptops, tablets); storage devices (e.g., USB and flash memory devices, CDs, DVDs, MP3 players, media storage servers); cameras (e.g., video and digital cameras and webcams); all types of mobile phones; gaming consoles, video and audio players/receivers (such as portable CD and DVD players); internet-enabled TVs (e.g. Google TV, Apple TV, SmartTV); any internal or external websites or web-enabled applications or systems used by the College in any way; and, any other similar technologies that currently exist or may exist in the future.

Implementation

Prevention

The College is responsible for sourcing and implementing relevant and developmentally appropriate programs and strategies that promote positive online behaviours and cybersafe practices. A range of classroom-based, interactive, online student learning, staff professional learning, and parent education opportunities will be utilised such as eSmart initiatives, cybersafety experts, promoting cybersafe websites, support materials and publishing relevant information via the College newsletter.

All staff, students and parents are responsible for acting in accordance with the College's annual ICT User Agreements, and to work in partnership to ensure the safe and productive use of ICT.

The College has the authority to monitor, access and review all College-based ICT usage by students, staff and parents. This includes emails sent and received on the College's devices and/or network facilities.

Intervention

Students, staff or parents can report any breaches of the ICT User Agreements or incidents of cyberbullying activity to their teacher as the primary cybersafety contact, or another staff member or the Principal at any time.

Any alleged incidences or allegations of behaviour that are in breach of the College's ICT User Agreement will be thoroughly investigated by the College.

Significant breaches made by, or involving, students will result in the College notifying the parents of those students.

The College's response to alleged breaches will be followed up with due diligence and consideration for all parties involved or affected by any breach.

The progress and well-being of any student involved in breaches will be monitored by the College when they are onsite at the College.

Where cyberbullying has been identified, support may be offered, as determined by the College.

Related Policies

Student Bullying Policy

Child Safety and Wellbeing Policy

Complaints and Grievance Policy

Digital Device Policy

ICT User Agreement

Related Legislation

Education and Training Reform Act 2006 (Vic)

Education and Training Reform Regulations (2017)

Approved College Leadership

Authorised College Executive