DIOCESE OF BALLARAT CATHOLIC EDUCATION LIMITED

ST JOSEPH'S SCHOOL COLERAINE

Digital Technologies Procedures

Definitions specific to these procedures

TERM	DEFINITION
Digital technologies	are defined as being any networks, systems, online services, software or hardware including electronic devices and applications that allow a user to access, receive, view, record, store, communicate, copy or send any digital information such as text, images, audio, or video. It includes the use of technology such as email, internet, intranet, phone, mobile device, social media sites, applications, online discussion and chat facilities, collaboration tools, copying and printing.
Grooming	is when a person engages in predatory conduct to prepare a child or a young person for sexual activity at a later time. Grooming can include communicating or attempting to befriend or establish a relationship or other emotional connection with the child or their parent or carer.
School environment	means any of the following physical, online or virtual places, used during or outside school hours: a) A campus of the School b) Online or virtual school environments made available or authorized by the School governing authority for use by a child or student (including email, intranet systems, software applications, collaboration tools, and online services) c) Other locations provided by the School or through a third-party provider for a child or student to use including, but not limited to, locations used for: ○ camps ○ approved homestay accommodation; ○ delivery of education and training such as registered training organisations, TAFEs, non-school senior secondary providers or another school; or sporting events, excursions, competitions or other events.

Actions

ACTIVITY	STEPS
General	• While staff, students and the school community will have access (as deemed appropriate) to electronic resources, this is a privilege not a right. • Users are responsible for ensuring that the resources are used in a purposeful, responsible, legal and ethical manner that is consistent with the diocesan vision. • Electronic resources are provided for work and education purposes. • Technology use will be monitored including the appropriateness of sites, material accessed, downloaded or distributed and communication utilised. • At all times child safety requirements and processes are to be considered in any use of technology. • All persons must sign the ***Acceptable Use and Cyber-safety Agreement***

Implementation

- All staff will receive training about online safety and be able to recognise and respond to online safety issues.
- Staff, students and parents must annually sign the ***Acceptable use and Cyber-safety Agreement*** each year in order to access the technology resources.
- All users are to comply with the policy and any diocesan and government legislation (such as Child Safety Standards, copyright, discrimination, defamation and privacy laws) in the use of technology.
- An audit of technology use will be conducted each term, or as required.
- Inappropriate material (including pornography) must not be accessed, downloaded, transmitted or posted.
- Communication and feedback between students, parents and staff via electronic media must be appropriate at all times.
- Electronic media must not be used for gambling purposes.
- Personal use for staff is restricted and limited. It must not take place during teaching or classroom time. Access must not interfere with work obligations or while supervising students (unless an emergency call to services or administration is required).
- Student and school community use is limited to educational use for engaging in student learning
- Email correspondence must contain the appropriate disclaimer.
- Downloaded files must be checked and be virus free.
- All digital content stored and produced remains the property of the employer.
- Privacy and confidentially must be considered in forwarding or providing access to electronic communication. Permission from the sender should be sought. Staff should ensure that personal information is kept private.
- Correspondence such as email is not necessarily kept confidential when sent to an external party and can be forwarded on or accessed by others without the writer's knowledge. It is important to check whether it is appropriate to send confidential information electronically.
- Communication via chat rooms, social media, email and text messages should always have appropriate content, images (if used) and language. They must not embarrass the organization's reputation or be construed as bullying or harassing, or embarrassing someone.
- Violation of the policy may include:
    - informing police after an initial investigation
    - For students: restriction or suspension of use for a set period of time or in the case of a serious breach suspension from school following appropriate procedures outlined in the Behaviour Management Policy
    - For parents/school community: restriction or suspension of use and access for a set period. In the case of a serious breach this may be permanent.
    - For staff: informing VIT (teachers) or performance/disciplinary processes that may lead to termination of employment.
- Regular reminders about acceptable use of technology will be communicated to staff and parents/carers via newsletters, bulletins and meetings.
- All school and CEB sites have a web filtering system in place to ensure inappropriate material cannot be accessed at school.

Learning and Teaching	• The learning environment must foster student confidence to report to staff if they have seen or received anything that has made them uncomfortable or threatened. This should always be followed up in a timely manner. • Learning and teaching practices, strategies and technologies are effectively incorporated into learning process and are used by teachers and students (see Learning and Teaching Policy). • Teachers have clear processes and practices and scaffold learning to manage classroom and online behaviour and respond appropriately to any incidents that may arise. • Teachers provide students with an understanding of appropriate sites and materials and a process to follow if an inappropriate site/material opens. • The School cannot filter Internet content accessed by a student from home, from other locations away from school or on mobile devices owned by students. The School recommends the use of appropriate Internet filtering software on such devices. • Teachers develop a curriculum scope and sequence for cyber safety that includes teaching safe, responsible and ethical online behaviours (see Duty of Care Policy, Anti-bullying [including cyberbullying] and Anti-harassment Policy). The scope and sequence is consistent with the Victorian government requirements for curriculum (see Learning and Teaching Policy). • Copyright and privacy laws and other legislation must not be breached in using the Internet and in posting material onto sites. • The leadership team will monitor the cyber safety curriculum and professional learning requirements for all staff. • Electronic teaching materials and sites used by teachers are to enhance learning and must be appropriate. • There will be regular communication to staff, students and school community on policies and procedures that foster a safe classroom environment. Information will be available on school website, Staff and Parent Handbooks. Teachers will also discuss issues and procedures with parents/carers in informal meetings and information nights. • Students will engage, as part of their learning, in using the internet which will include accessing sites such as websites, electronic chats (social media), bulletins, educational apps and classrooms (such as Google Classroom) and the use of email. • Teachers will provide guidance as to which sites can be accessed and programs that can be downloaded on to school devices. Teachers will develop processes for students to follow if they access an inappropriate site or are confronted with material or text that makes them uncomfortable. • Teachers will use educational resources such as the Office of Children's eSafety Commissioner at https://www.esafety.gov.au/ to develop student knowledge, skills and capabilities in cyber safety. • Students must not post any inappropriate texts or images or engage in bullying or harassment through the use of these sites or in using email. Students must not download any unauthorised programs. • Schools use Google Classroom. Teachers at all times will engage in a professional manner in responding to student messages, student work and in providing appropriate materials. • Parents will be provided access to Google Classroom to communicate with teachers and view their own child's work and feedback. Parents at

	all times must communicate appropriately when using this or other modes of communication with the School. • All families receive a copy of the Digital Technology: Acceptable Use and Cyber Safety Agreement annually. Parents are asked to read the agreement with their children and sign the agreement. This is returned to the School (Refer also to Anti- bullying and Anti- harassment Policy).
School electronic equipment and devices	• Students are expected to use school equipment and devices safely and with care. • Teachers will induct students on how to safely use and look after any electronic equipment or device. • Students must not download programs on to school equipment or devices without the permission of the teacher. • The device must be returned the next day to the teacher and must be fully charged. The student is not permitted to download any programs onto the device or access inappropriate sites. It can only be used for the educational purpose for the loan. Teachers must check the device when it is returned; that it is not damaged or has unauthorised programs/apps on it.
Social Media	• The use of social media is used by members of the school community as a social tool and is commonly used to express views, comments, and ideas on a range of issues. • Students, as part of the educational program, will engage, from time to time, in electronic chats to share their learning, pose questions and provide feedback to other students. This interaction may occur with students within their own classroom, classes in the School or students in another school. • Teachers will have access to these sites and will monitor that the content is appropriate and that students are not engaging in anti-social behaviour such as cyberbullying. • Teachers are not permitted to engage in other social media (non-school) where students participate. • It is expected that all members of the school community when engaging with each other through using social media behave in such a manner that: o the welfare of all members of the School is not adversely impacted upon. o the reputation of the School is not negatively affected or brought into disrepute o personal information is kept private o uploading or posting inappropriate content on any space or sight does not occur. • Social media sites (other than those established for student learning under the supervision of a teacher) utilising the School name must not be established, unless the principal gives permission. This permission would only be for a specific school purpose. If the site is not used appropriately according to the requirements for its use, it will be closed down. • When using social media, it is expected that members of the school community will: o demonstrate appropriate personal and professional boundaries and behaviours

	○ ensure online behaviour reflects the same standards of honesty, respect, and consideration that a person uses when communicating face-to-face ○ respect the rights, privacy and confidentiality of others. ○ ensure all content published is accurate and not misleading ○ not post or respond to material that is offensive, obscene, defamatory, threatening, harassing, bullying, discriminatory, hateful, threatening, violent, racist, sexist, pornographic, or is otherwise unlawful. ○ not infringe on copyright or cause damage to the reputation of the School, or bring it into disrepute.
Mobile Phones	Mobile phone use is not permitted at school unless expressly authorised by the Principal. Any mobile phones brought to school are the responsibility of the child and any damage or loss will be borne by the student. They must remain in the student's personal belongings and not be used at school. Any breach will be managed by the Principal.

Supporting Documents

Related DOBCEL Policies and Procedures

- Digital Technology Procedures
- Assessment and Reporting Policy
- Duty of Care – Supervision of Students
- Learning and Teaching Policy
- Child Safety & Wellbeing Policy
- Privacy Policy
- Behaviour Management Policy
- Bullying Prevention (including Cyberbullying) [Students] Policy

Forms, Templates and Associated Documents

- Acceptable Use and Cyber-safety Agreement

Approving authority	DOBCEL Board
Approval Date	December 2025
Review Date	December 2028