ACCEPTABLE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY POLICY

1.0 PURPOSE

Diocese of Sale Catholic Education Ltd (DOSCEL) recognises the importance of digital technologies in supporting teaching and learning. Information and Communications Technology (ICT) supports effective teacher practice and curriculum delivery. All DOSCEL schools support students to be confident and safe users of ICT. All schools will promote and educate children in cyber safety.

2.0 PRINCIPLES

2.1 ICT supports teachers to deliver the curriculum and target teaching to address the needs of all students.

2.2 Access to ICT supports students to be confident users of digital technologies.

2.3 The use of ICT requires safe, ethical and respectful communication and collaboration ensuring every child and young person's safety.

2.4 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 online learning environments.

2.5 A whole school approach is the most effective way to support the use of ICT and to ensure cyber safety.

2.6 School practice in the use of ICT will be informed by the Australian Government eSafety Commissioner.

3.0 DEFINITIONS

3.1 **Cyberbullying** is when a child or young person is threatened, harassed, humiliated, embarrassed or targeted by another person using the internet, mobile phone, instant messaging, e-mail, chat rooms and social networking sites such as Facebook and Twitter, or any other type of digital technology.

3.2 **Digital technologies** are electronic tools, systems, devices and resources that generate, store or process data.

3.3 **Digital learning** is any type of learning that utilises digital technology.

3.4 **Applications (Apps)** are software programs that run on a computer or mobile device. Web browsers, e-mail programs, word processors, games and utilities are all applications.

4.0 USE OF ICT

4.1 **ICT Applications** - Students access endorsed applications to support learning, collaboration and information sharing. Student work may be shared between teacher and student, student and student, student and parent, and with permission, within the broader school community. When sharing work teachers will ensure that students understand and observe protocols and procedures. The work shared, including images, videos and presentations remain the property of the school and cannot be copied, published or distributed in any other forum, without permission.

4.2 **Cloud Storage** – DOSCEL schools may utilise cloud storage solutions (such as Google Drive and Microsoft 365) for the storage of documents and presentations. Cloud storage enables collaboration among staff and students, and provides ready access to information across multiple devices. DOSCEL ICT services, in partnership with schools, provide managed access to cloud based applications through the use of usernames and passwords. Considerations when accessing school resources outside of the school environment include:

- the use of secure, safe and reliable internet connections
- safe and appropriate storage of important documents
- a safe internet browser free of viruses and a virus-free device
- the use of secure username and passwords.

4.3 **School Email** - Students have an assigned school email address. Students have a responsibility to use their school email appropriately and in accordance with school expectations of appropriate use of ICT. The student email is not permitted to be used for online transactions, participating in forums or for accessing third party applications for personal, outside of school, use.

4.4 **Digital Media** – Students may be provided with access to digital media i.e. online text, audio, video and graphics which supports the delivery of curriculum.

5.0 ACCEPTABLE USER AGREEMENT

5.1 DOSCEL schools will develop an *Acceptable User Agreement (AUA)* for all students to sign. The *AUA* will include:

- A school profile statement describing how the school educates students to be safe, responsible and ethical users of digital technologies.
- An educational rationale outlining the technologies and approaches the school is using to support student learning with digital technologies.
- Schools will include a list and description of the online services they are using, and describe their approach to managing students' personal information and data.
- A student declaration outlining the conduct expected of students when using digital technologies.
- An acknowledgement section for students and parents to declare their understanding of the AUA by providing their signature.
- Signed consent where parents grant permission for students to use applications and services based on age restriction and Australian broadcasting classifications e.g. YouTube.

6.0 PROCESSES AND PROCEDURES

6.1 DOSCEL will:

- Provide advice to schools in relation to the safe and effective use of ICT.
- Support schools in the management and deployment of ICT resources.

6.2 Principals will:

- Adopt and implement the *Acceptable Use of ICT Policy*.
- Support DOSCEL policies and procedures supporting the safety, welfare and care of students when online.
- Use a whole school approach to determine the use of ICT.
- Develop a whole school approach to cyber safety education.
- Develop and implement an *Acceptable User Agreement* for students.
- Respond promptly to any inappropriate use of ICT.
- Ensure staff understand and implement the DOSCEL *Behaviour Management Policy, Cyber-Safety Policy* and *Anti-Bullying and Bullying Prevention Policy* to effectively manage inappropriate use of ICT.
- Regularly communicate this policy to staff and promote the importance of cyber safety for all.
- Provide the community with access to cyber safety information via the Australian Government eSafetyCommissioner.

6.3 School staff will:

- Support DOSCEL policies and school-based procedures.
- Create and maintain safe access to ICT for students.
- Ensure student supervision when online.
- Ensure that the use of ICT is exclusive to the implementation of the curriculum and supporting the progression of learning of students.
- Address cyber safety in line with the whole school approach.
- Manage content accessed based on Australian classifications and age restrictions. (Refer to the Australian Government Australian Classification and the eSafetyCommissioner – eSafety Guide).
- Manage inappropriate use utilising appropriate policies and procedures, including the DOSCEL *Behaviour Management Policy, Cyber-Safety Policy* and *Anti-Bullying and Bullying Prevention Policy*.
- Participate in appropriate professional learning and training supporting the care, safety and welfare of students online.

6.4 Students will:

- Abide by school policies and procedures.
- Cooperate with staff in ensuring a cyber-safe environment.
- Sign and abide by the *Acceptable User Agreement*.
- Contribute positively to the development of safe and inclusive online learning environments.
- Appropriately report incidents of cyber bullying.
- Maintain device settings ensuring device access, integrity and security is not compromised.
- Ensure they do not share usernames or passwords.

6.5 Parents and carers will:

- Sign and support the *Acceptable User Agreement*.
- Report incidents of cyber bullying to the classroom teacher/principal.
- Work in partnership with schools to ensure the safety of students in the online environment.
- Support DOSCEL policies and school-based procedures.
- Support students through the creation of an eSafe home environment. For further advice parents are encouraged to access the Australian Government eSafetyCommissioner Parent Portal.

7.0 EXPECTED OUTCOMES

7.1 Every Catholic school in the Diocese of Sale implements the DOSCEL Acceptable Use of ICT Policy.

7.2 Every student will have a signed Acceptable User Agreement.

7.3 School community members work respectfully and collaboratively in support of a cyber-safe online environment.

8.0 RELATED POLICIES

- Anti-Bullying and Bullying Prevention Policy
- Behaviour Management Policy
- Pastoral Care Policy
- Privacy Policy

9.0 REVIEW

Implementation Date: June 2022

Review Date: June 2025