St Francis Xavier College
Berwick, Officer and Beaconsfield

Procedure for

Digital Learning

St Francis Xavier College procedures are designed to enable the College to enact the policies of the Diocese of Sale Catholic Education Limited (DOSCEL).

All College Procedures intentionally promote a child safe culture which prioritises the safety and wellbeing for all students.

Contents

Purpose

The purpose of this Procedure is to support students to engage in online environments, using digital technologies, in a safe and responsible way.

DOSCEL schools are committed to providing safe and secure learning environment for all its students. Schools recognise the importance of digital technologies as a learning tool and are committed to reducing students' exposure to online/cyber risks, whilst also developing students as responsible online/cyber citizens who demonstrate ethical behaviour when using online and digital technologies.

St Francis Xavier College Procedures are designed to enable the College to enact the Policies of the Diocese of Sale Catholic Education Limited (DOSCEL).

Scope

This procedure applies to all members of the College community.

A whole school approach is used to develop a culture of safety and to prevent risks to online safety.

Definitions

Acceptable Use Policies	Acceptable Use Policies are documents created by education systems or schools to outline what is acceptable behaviour when using computer facilities and other technologies such as mobile phones.
Online Safety or 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.
Online abuse or cyber abuse	Online abuse is 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.
Explicit material	Explicit material means any drawing, photograph, film negative, motion picture, figure, object, novelty device, recording, transcription or any book, leaflet, pamphlet, magazine, booklet or inline service, the cover or contents of which depicts human genitalia or depicts or verbally describes nudity, sexual activity, sexual conduct, sexual excitement or sadomasochistic abuse in a way which is harmful to minors. Explicit material does not include any depiction or description which, taken in context, possesses serious

	educational value for minors or which possesses serious literary, artistic, political or scientific value.
Illegal and restricted material	'Illegal and restricted material' refers to content that ranges from the most seriously harmful material such as images and videos showing the sexual abuse of children or acts of terrorism, through to content that should not be accessed by children, such as simulated sexual activity, detailed nudity or high impact violence.
Inappropriate content	Inappropriate content is 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 explicit material. Young people may encounter inappropriate content accidentally or deliberately.
Grooming	Grooming is 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.
Image-based abuse	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.
Online bullying or cyber bullying	Online bullying is the ongoing abuse of power to threaten or harm another person using technology. Cyber bullying can occur in chat rooms, on social networking sites, through emails or on mobile phones and includes abusive texts and emails, hurtful messages, images or videos, imitating others, excluding others, humiliating others, spreading nasty gossip and chat, and creating fake accounts to trick someone or humiliate them.
Scams	Scams are dishonest schemes that seek to take advantage of people to gain benefits such as money or access to personal details.
Sexting / Sharing nudes	'Sexting', commonly known as sharing a nude or a naked selfie, is the sharing of a sexually explicit picture or video via mobile phones, instant messaging apps, and/or social media sites. With modern technology this can be done instantly, it could also involve sharing between devices which work offline.

Trolling	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.
Unwanted contact	Any type of online communication that a person finds unpleasant or confronting, or that leads them into a situation where they might be harmed. This could include harassment, attempts to contact on multiple platforms, regular instant messaging, and more.

Procedure

1. Identifying Risks and Prevention of Online Abuse

New technologies / digital platforms (including software, apps and online surveys)

Risk assessments help to identify areas of risk and inform the College on the best technologies to use and any risk mitigation strategies that may be necessary.

Consideration should be given to:

- How and where is personal information or other data stored and shared?
- Is the platform bound by Australian Privacy Legislation?
- Are there location services that can identify the location of a child?
- Can students access inappropriate content on this platform?
- Does the platform have a minimum age requirement?
- Are staff familiar with how to use the platform safely?
- What training materials are available for staff and students?
- Should parents provide individual informed consent of this platform?
- Is misuse reportable and/or moderated?
- Are there appropriate privacy settings?

The College network provides all students and staff with a secure internet connection. All internet activity is monitored and filtered to meet all child safety standards.

The following sites are blocked for all students

- All social media sites (Facebook, Instagram, Twitter etc.)
- All social chat services (Discord, Google Chat, etc.)
- All entertainment streaming services (Netflix, Stan, Disney+, etc.)
- All malware site (unsecure or shareware download sites)
- All adult rated sites

As new online services become accessible, staff regularly identify new and emerging sites or services that can be flagged as inappropriate.

College firewalls and restrictions (filters, alerts, etc.)

Risk mitigation strategies include the use of a variety of relevant restrictions which help to identify, reduce, or remove risk factors.

The College has instigated the following:

- Tools to monitor or filter harmful content (Eg; Sassyan Assure monitoring service) for the purpose of monitoring areas such as:
  - Profanity and Sexual Language
  - Cyber Bullying
  - Self-harm

  All student online activity is monitored under these areas – both web activity and online communication (TEAMS, email etc.)

- Tools to share alerts with key staff. Daily alerts are pushed to each Head of House and Senior Pastoral Leaders summarising the alert categories. All alerts are sent to the Senior Leader and Directors of the Network Team

- College firewall (Eg: Palo Alto) to filter all network traffic
  - Internet
  - Email
  - TEAMS

  The firewall blocks all inbound and outbound traffic that is flagged as “inappropriate”. Only whitelisted activity is allowed on the College Network.

Supervision when using digital technology in the classroom

Active supervision (from staff) relating to the use of digital technology in the classroom included (but is not limited to):

- moving around the room to regularly monitor screens
- installing remote access software that enables teacher access to individual students’ 1 to 1 learning device used in class (eg: LAN school)
- actively communicating and reinforcing learning and behavioural expectations during the activity

2. Communication, awareness raising, and education related to online safety

Communication, awareness raising, and education may take the form of:

- Information sessions (face to face or online)

- Emails
- Links to resources
- Links to external awareness or learning sessions

Communication, awareness raising, and education may include topics such as:

- Privacy and security settings
- Digital Reputation
- Rights under the privacy act
- Unwanted contact
- Inappropriate content
- Explicit or illegal content
- Online/cyber bullying
- Sexting / sharing nudes
- Image based abuse
- Know and identify “Connected Devices”
- Apps and services
- Sharing images of fights
- Child pornography laws

3. Responsible online behaviours

The College device must be used in line with the College’s Digital Learning Program Agreement.

Students and staff are expected to use digital technology and online forums in a manner that upholds the College’s values, policies and procedures.

In particular, the following are relevant:

- DOSCEL Anti-Bullying and Bullying Prevention Policy
- DOSCEL Child Safety Policy
- DOSCEL Suspension, Negotiated Transfer and Expulsion Policy
- DOSCEL Acceptable Use of ICT Policy
- DOSCEL Behaviour Management Policy
- DOSCEL Child Protection Policy
- DOSCEL Child Safety Code of Conduct
- DOSCEL Pastoral Care Policy
- College Pastoral Care and Positive Behaviour Support Guidelines
- College Child Safety Program
- College Wellbeing Guidelines
- College Digital Learning Program Agreement
- College Personal Mobile Device Procedures

4. Reporting Online Safety Concerns

The College encourages students to take action when they have been involved in an online incident:

- Ask for the content to be removed
- Block the sender of the content
- Report the issue (to the school, local police and/or e-safety)

Students are also encouraged, and have access, to use a Bully Alert Form to report incidents to the College.

Reporting to the College

The College uses the Recognise, Respond, Refer model to encourage awareness and help-seeking amongst students.

Recognise: the signs that you or a friend may need help
Respond: by talking to your friend about what you have noticed, and your concerns
Refer: by getting help from a trusted adult

Students can report an incident to any staff member, particularly their Care Group Teacher, Head of House, or a member of the College Counselling Team.

Reporting to eSafety

eSafety helps Australians prevent and deal with harm caused by serious online abuse or illegal and restricted online content.

Reports can be made to the safety commissioner via the eSafety website: Report online harm | eSafety Commissioner.

Reports need to be made by the person who has experienced the abuse or received the illegal or restricted content. The College can support this report with the consent of the person.

Reporting to relevant authorities

All serious and potentially criminal activities can be reported to the Victoria Police.

All incidents that involve the sexual or physical abuse of a child (including sexually explicit material or child pornography material) must be managed in accordance with legislative requirements and the College's Child Protection Policies and Procedures and reported to Victoria Police and the Department of Fairness, Families and Housing Child Protection.

5. Responding to concerns

Online interactions that breech the College's behavioural expectations will be managed in line with the College's Positive Behaviour Support Procedure. This is regardless of whether the interaction took place during school hours or outside of school hours where it involves students from the school.

Tier 1 and 2 online antisocial behaviours include:

- Teasing, name calling and put downs
- Meme posts that put down others
- Social exclusion
- Unwanted contact

Note: The persistence of Tier 1 and 2 behaviours could move them to a Tier 3 behaviour.

Tier 2

- Impersonation and fake accounts
- Sharing images of fights or violence
- Sharing inappropriate sexualised messages

Note: The persistence of Tier 1 and 2 behaviours could move them to a Tier 3 behaviour.

Tier 3 online antisocial behaviours (serious and potentially criminal behaviours) include:

- Hate speech, discrimination and sexual harassment
- Incitement to suicide or self-harm
- Threats to physical harm
- Non-consensual sharing of intimate images
- Capturing and sharing images of staff
- Online grooming

In responding to these behaviours, the College will consider the following:

- The nature and severity of the interaction or behaviour
- The frequency of the interaction or behaviour
- The impact of the interaction or behaviour

In responding to these behaviours, the following steps guide staff actions:

1. Understand and assess the situation/incident
2. Manage a response
3. Work to resolve the conflict or respond to the issue
4. Record and reflect
5. Monitor that the incident has resolved

For Tier 3 incidents, the following will also be actioned:

- Supporting safety and wellbeing (both immediate and long term)
- Collection and recording of evidence (where possible – noting that some illegal material such as child abuse material cannot be collected)
- Removal of content
- Reporting to relevant people and authorities

These steps are informed by:

- Appendix 1: Online Incident Assessment Tool (from eSafety Commissioner) (Appendix 1).
- Quick reference guides for responding to online safety incidents (from eSafety Commissioner) (Appendix 2).

6. Resources and advice

The following website contains information for the community which promotes online safety and/or offers support for young people impacted by the misuse of digital technology:
ESafety Commissioner

The eSafety Commission is the leading resources in:

- awareness and prevention of online abuse
- support following misuse of digital technology or online forums

Learning resource materials

- Digital Thumbprint – DT
- ACSC Homepage | Cyber.gov.au
- Cyber Safety Project

7. Record Keeping

Instances of significant breeches of the College's Positive Behaviour Support expectations are recorded
in SIMON.
All instances of reported online anti-social behaviours should be noted in the SIMON Student Profile as an Incident or (where relevant) follow the College's process for record keeping relating to Suspension

Compliance

Key Responsibilities

Employee Responsibility

All employees and volunteers are responsible to:

- Model appropriate behaviour at all times
- Act in accordance with the Child Safe Code of Conduct
- Manage all reported and observed incidents of online bullying in accordance with the Bulling Prevention and Intervention procedures

Relevant Legislation

- Education and Training Reform Act 2006 (Vic)
- Privacy and Data Protection Act 2014 (Vic)
- Online Safety Act 2021 (Au)

Related DOSCEL Policies

- DOSCEL Anti-Bullying and Bullying Prevention Policy

- DOSCEL Child Safety Policy
- DOSCEL Suspension, Negotiated Transfer and Expulsion Policy
- DOSCEL Acceptable Use of ICT Policy
- DOSCEL Behaviour Management Policy
- DOSCEL Child Protection Policy
- DOSCEL Child Safety Code of Conduct
- DOSCEL Pastoral Care Policy

Related College Procedures

- College Pastoral Care and Positive Behaviour Support Guidelines
- College Child Safety Program
- College Wellbeing Guidelines
- College Digital Learning Program Agreement
- College Personal Mobile Device Procedures

Review & Evaluation

Review occurs every two years.

Further Information

Further information can be obtained from: Deputy Principal Wellbeing

Status of Procedure	
College Leader Responsible	Deputy Principal Wellbeing
Implementation Date / Last Reviewed	March 2024
Review Date [Commonly 1 – 2 Years]	March 2026
Local Governing Authority Approval	College Executive team

Record of Review

Details of Amendments	By Whom	Date
New	Deputy Principal Wellbeing	July 2022
All areas reviewed and current	Deputy Principal Wellbeing	March 2024

Appendix 1: Online Incident Assessment Tool
respond_1_-_online_incident_assessment_tool.pdf (esafety.gov.au)
Appendix 2: Quick reference guides for responding to online safety incidents
Respond | eSafety Commissioner