Melbourne Archdiocese Catholic Schools

Checklist for Suspected ICT Breaches – Students

Template for School use

St James the Apostle Catholic Primary School

Melbourne Archdiocese Catholic Schools Ltd (MACS) schools are responsible for developing safe, inclusive, and respectful learning environments, including online environments which maintain student digital responsibility and citizenship.

The checklist is designed to support schools as they investigate suspected student ICT breaches, to assist in meeting their compliance and obligations regarding the following legislation and MACS policies:

- Child Safe Standards
- *Online Safety Act 2021* (Cth)
- *Online Safety Amendment (Social Media Minimum Age) Act 2024*
- MACS ICT Acceptable Use Policy – Students
- MACS Child Safety and Wellbeing Policy
- MACS Student Behaviour Support Policy
- MACS Steps to Review a Student Device procedure
- MACS Bullying Prevention and Response Policy
- MACS eSafe Behaviours
- eSafety education: online incident assessment tool

The checklist is intended to guide schools in adopting a fair, restorative approach wherever possible, when investigating a suspected student ICT breach.

ICT breaches may include, but are not limited to, the following that may occur during or out of school hours:

- academic misconduct (i.e. plagiarism, cheating, copying, sharing, etc.)
- online behaviours that may cause harm such as:
  - cyberbullying or harassment
  - sharing or creating material that is explicit, illicit, or harmful
  - use of deep fake or AI tools to impersonate (via image, video or sound), humiliate, or defame
- misuse of school devices or digital tools or attempts to bypass network security or filters.

School: Click or tap here to enter text.

Student(s) involved: Click or tap here to enter text.

Type of breach: Click or tap here to enter text.

Date and Time: Click or tap here to enter text.

Leaders/Teachers reviewing breach: Click or tap here to enter text.

Breach classification	Y/N	Out of hours Y/N	Date	Leadership Initial
1. Academic misconduct				
2. Cyberbullying				
3. Deep Fake				
4. Social media breach (Code of Conduct)				
5. School network/ security				
6. Other				

Possible Actions	Affected Party/Parties	Perpetrator(s)
Refer to relevant policies, as relevant to the incident, including: ● ICT User Agreement Policy ● Student Code of Conduct. ● School Academic Honesty Policy, and/or ● VCE/VPC Administrative Handbook.	☐	☐
Discuss alleged incident with suspected perpetrator(s), providing opportunities to respond to allegation(s) and record incident on the school LMS.	☐	☐
Communicate to all affected parties that an allegation has been made and that an investigation will be conducted, as applicable.	☐	☐
Use the eSafety education online incident assessment tool to evaluate scale and impact of the incident and record evidence.	☐	☐
Where instance involves suspected network breach, review network security and impact of suspected breach. Record evidence.	☐	☐
Once breach is confirmed, inform all relevant parties that further steps will be taken, as appropriate.	☐	☐
Remove network / device access, if applicable.	☐	☐
Support safety and wellbeing of affected party(ies): ● Prioritise and support throughout the entire process. ● Refer to Student Engagement for student wellbeing support as and if necessary. ● Make and maintain contact with affected party(ies)' parents and relevant staff. Refer parents to the support of eSafety commissioner if necessary.	☐	☐
Principal to decide on consequence(s).	☐	☐
Communicate consequence(s) with relevant student(s), parents and staff. Provide student(s) with opportunities to respond/appeal, if applicable.	☐	☐
Support all students' safety and well-being following assignment of consequence(s).	☐	☐
Record incident on school bullying register, if applicable.	☐	☐
Inform senior manager, school leadership (SMSL) if school will require contact with Victoria Police, MACS Legal, Student Engagement, and Child Safety teams.	☐	☐
Depending on scale and impact, report to Victoria Police.	☐	☐
If incident has spread beyond relevant party(ies), communicate with school staff, affected class, year level and parents/carers promptly to confirm incident is known and managed.	☐	☐

Suggested consequence guidance – Please highlight or document consequence under the table

Breach	1st Incident	2nd Incident	3rd Incident
Academic misconduct (i.e. plagiarism, cheating, copying, sharing, etc.)	Contact with family – loss of marks/ school behaviour system eLearning assigned as a proactive measure	Family meeting – loss of marks/ school behaviour system	Suspension 1 day – loss of marks/ school behaviour system
School network/ security	Contact with family *Removal of device eLearning assigned as a proactive measure	Family meeting *Removal of device	Family meeting *Suspension external/ internal
Deep Fake (digital - image, voice, video, other)	Family meeting with (potential for suspension 1 -3 days*)	Family meeting with (potential for suspension)	Extended suspension that is in correlation with the breach – Enrolment discussion
Social media breach (Code of Conduct)	Family meeting with potential for suspension (1 – 3 days*)	Family meeting with potential for suspension (1 – 3 days*)	Family meeting with potential for suspension (1 – 3 days*)
Out of hours breach; action at Principal discretion	Family meeting with potential for suspension/ loss of access (1 -3 days*) eLearning assigned as a proactive measure	Family meeting with potential for suspension/ loss of access (1 – 3 days*)	Family meeting with potential for suspension/ loss of access (1 – 3 days*)
Other; action at Principal discretion	Family meeting with potential for suspension (1 -3 days*) eLearning assigned as a proactive measure	Family meeting with potential for suspension	Family meeting with potential for suspension

- Consequence assigned: _____
- SMSL contact
- Community Management
- Media management

Possible school actions:

- Family contact made following the breach
- Victim supported with follow up meetings as required by their needs
- Re-entry meeting held for suspended students – support offered for their needs
- Bullying register updated
- Copy of breach report included in student file
- Staff debrief using school emergency management debrief procedure
- Staff affected by the breach offered support via the appropriate resource at the discretion of the Principal
- e-safe learning curriculum adjusted to include additional support as required
- e-safe messaging item in the school newsletter in the week following the incident – draw on eSafety Commission resources for additional support.