VPS Staff Procedure for Responding to Moderate Cyber Incidents Affecting Students

Step 1

Identify Concern

Talk to and discuss the incident with all parties , if it is one of the scenarios below proceed with this flow chart.

If not turn over to the Severe Incident flow chart.

<u>If unsure see the Digital Technology Teacher or one of the Principals.</u>

⇒ Making general negative comments online
⇒ Plagiarism
⇒ Using or sharing Passwords
⇒ Inappropriate language online
⇒ Searching for content that is inappropriate or illegal
⇒ Posting our own personal information online (see AUA)
⇒ Having 'underage' social media accounts

Step 2

Take Action

Ensure all students are safe

Record details from all involved – this may include all staff and students who may have been directly or indirectly involved in the incident and/or its effects

Keep any evidence –

eg. screenshots, emails, texts etc

Step 3

Respond

Refer to the relevant Acceptable Use Agreement and discuss how the 'incident' is a breach of this

Contact Parents of all students (including witnesses in a manner that suits in the incident.)

Step 4

Consequences

Write, explaining how they have breached the Student Agreement and what its impact was on others

Warning for first time or unintentional offence

OR

Restricted use of technology for a short period of time

Education targeted at year level where appropriate

Step 5

Record

Create a chronicle entry on COMPASS to document a Cyber Incident.

Make sure to record the steps taken to resolve the incident
eg. steps taken to remove content, mediation attempts

Notify classroom teacher

eSmart®

VPS Staff Procedure for Responding to Severe Cyber Incidents Affecting Students

Step 1

Identify Concern

Talk to and discuss the incident with all parties , if it is one of the scenarios below proceed with this flow chart.
If not turn over to the Moderate Incident flow chart.

<u>If unsure see the Digital Technology Teacher or Principals.</u>

- ⇒ Damaging ICT Equipment
- ⇒ Making negative comments online targeting an individual or specific group
- ⇒ Identity Theft
- ⇒ Stealing passwords or using another individual's password for inappropriate or malicious use
- ⇒ Work or images that personally attack, humiliate or defame an individual
- ⇒ Posting other people's personal information online (see AUA)
- ⇒ Having 'underage' social media accounts without parent/guardian knowledge
- ⇒ Accessing or attempting to access inappropriate content.

Step 2

Take Action

Ensure all students are safe

Record details from all involved – this may include all staff and students who may have been directly or indirectly involved in the incident and/or its effects

Keep any evidence – eg. screenshots, emails, texts etc

If the incident is found to be a criminal act, notify Parents and police ASAP after consulting with Principals.

Step 3

Respond

Provide reasonable & ongoing wellbeing support to all students & staff who were involved in or witness to the event.

Refer to the relevant Acceptable Use Agreement and discuss how the 'incident' is a breach of this.

Where relevant work with families, social media/game/messaging sites to take down inappropriate/ offensive material.

Contact Parents of all students, including witnesses

Step 4

Consequences

Write, explaining how they have breached the Acceptable Use Agreement and what its impact was on others

Warning for first time or unintentional offence

OR

Restricted use of technology for a short period of time

Education targeted at year level where appropriate.

Step 5

Record

Create a chronicle entry on COMPASS to document a Cyber Incident.

Make sure to record the steps taken to resolve the incident eg.
steps taken to remove content, mediation attempts

Notify classroom teacher

Notify student welfare co-ordinator

eSmart®