Kororareka Russell School

Responding to Digital Incidents

At Kororareka Russell School we have clear guidelines about acceptable and unacceptable use of technology; and students, caregivers, and parents sign use agreements. We take any breach of cybersafety seriously and respond as appropriate.

A major digital incident such as the posting of highly personal information or a graphic photo/video online can have a significant impact on students and staff. The school has the authority and responsibility to act, even when the incident takes place outside of school.

If damaging content has been posted online or a staff member or student has been involved in a scam, the school acts to minimise student/staff distress and ensure their safety. We follow our policy for the **surrender and retention of digital devices**, and we apply our **behaviour management** strategies in cases of unacceptable student behaviour such as cyberbullying.

In response to a digital incident, the school will:

- gather the facts to determine what has happened and who is involved
- support the students/staff involved
- determine the nature of the content (is it illegal, threatening or intimidating, objectionable, or does it breach privacy?)
- get offensive or inappropriate online material removed if possible:
  - ask the person responsible to remove the offending information, page, or website
  - request that the service provider or website owner remove the information or page
- seek advice from other organisations if necessary, e.g. Netsafe, the ▶**Ministry of Education's traumatic incident team**, and/or the police
- support those affected by the digital incident, where appropriate, to use "report abuse" buttons or other feedback methods on websites to report abuse/bullying, or report inappropriate text messages to the relevant service provider
- contact other relevant parties, e.g. senior staff, the board, pastoral staff, or parents/caregivers
- determine how/when to release information to the wider community and the **media**
- record full details of the incident.

If the school was the online content host, the school uses the ▶**safe harbour** process as detailed by the Ministry of Justice, and/or seeks legal advice as necessary.

After the incident is resolved, the school continues to monitor the wellbeing of the affected students/staff and provides support if needed. The school holds a debrief to assess management of the incident, and how well the **cybersafety guidelines** were implemented.

See Netsafe's 📕 **Responding to Online Digital Incidents Involving Students** for comprehensive information and guidelines, and quick links for reporting breaches to popular social media sites.

Related topics

- **Digital Technology and Cybersafety** ☑

- **Bullying** ✅
- **Cyberbullying** ✅
- **Privacy** ✅

Legislation

- Harmful Digital Communications Act 2015
- Privacy Act 2020

For other relevant legislation, see 🌐 **Netsafe's overview of legislation relevant to digital technology**, broken down by type of digital incident.

Resources

- Netsafe: **Incident Support** 🌐
- Ministry of Education: **Digital Technology: Safe and responsible use in schools** 🌐
- Ministry of Education: **Traumatic Incidents: Managing student and staff wellbeing** 📄
- Ministry of Justice – **Safe harbour provisions** 🌐

Release history: **Term 2 2020**

Last *scheduled review*	
Last *internal review*	*Term 2 2020*
Topic type	*Core Generic*