



Te One School

Currently under review

We are reviewing this policy for its content and how well the school implements it. To share your comments and rate its implementation, click the "Start your review" button.

About the review process

[Start your review](#)

Responding to Digital Incidents

See [Computer Security and Cybersafety](#) for our procedures for managing cyberattacks, data breaches, or other computer security threats.

Incidents involving digital technology may negatively affect the learning environment or impact the emotional or physical safety of our school community. Te One School responds appropriately if there is reason to believe that our digital technology and online safety policy has been breached or an incident involving digital technology has occurred (Education and Training Act 2020, Health and Safety at Work Act 2015, Harmful Digital Communications Act 2015). We also respond to concerns and incidents that take place outside school but have an impact on the school community.

We encourage anyone who may have concerns or information about a digital incident to inform the school. We act immediately to minimise distress and harm, safeguard the safety and wellbeing of those affected, and help to resolve the matter as soon as possible. Digital incidents may vary in their nature and severity, and may involve students, staff, and/or others. Appropriate staff manage digital incidents according to the situation, in consultation with senior management and the board, as appropriate. This may include clarifying roles and responsibilities to ensure the most effective response.

Responding to a digital incident

Our school may need to respond to a wide range of digital incidents, including breaches to our digital technology use agreements, [▶ online bullying](#), personal information breaches, and inappropriate content. How we respond depends on the nature of the incident and whether students, staff, and/or other members of our school community are involved. We are guided in our response by the **Digital Technology: Safe and responsible use in schools guide** created by the Ministry of Education and Netsafe (see [Resources](#) below).

If the school believes a digital incident has occurred, we:

- determine what has happened, who is involved, and who owns the digital technology/content involved in the incident
- assess the [▶ nature of the incident](#)
- maintain the integrity of digital devices, the information stored on them, and any online content that may be required as evidence
- [▶ seek support and report incidents](#) as appropriate
- use the [▶ safe harbour](#) process and/or seek legal advice as necessary if the school was the online content host

- determine how/when/whether to release information about the incident to the wider community and the **media**.

If students are involved in a digital incident we may follow our **Behaviour Management, Bullying and Harassment**, and **Surrender and Retention of Personal Digital Devices** policies as appropriate. We contact and collaborate with parents/caregivers and whānau as needed. If students at another school are also involved with the digital incident we work with the other school to resolve the situation and support our school communities.

If staff or other members of the school community are involved in a digital incident we may follow our **Staff Conduct, Concerns and Complaints Policy, School Community Conduct Expectations**, and **Bullying and Harassment** policies and procedures, as appropriate.

Our school processes for **privacy and confidentiality** are followed at all times. See **Privacy**.

Support

We respond to concerns and incidents with care and caution. For students, this includes pastoral care and connections to external support, as needed. For staff, this may include access to an employee assistance programme or external support. Also see **Responding to Student Wellbeing Concerns** and **Staff Wellbeing and Safety**.

We recognise that a digital incident can be traumatic for students, staff, and our school community and may require us to activate our crisis management plan. After the incident is resolved, the school continues to monitor the wellbeing of those affected and provides ongoing support as appropriate.

Recording and storing information

We record full details of the incident (including all decisions and actions taken) in our school management system. This includes documenting concerns, conversations, incidents, contact with parents/caregivers or external agencies, advice received, actions taken (including rationale), and any follow-up, support, or monitoring plans.

The school debriefs the incident to assess how processes could be improved and how we can prevent similar incidents.







Related policies

- **Supporting Student Wellbeing**
- **Child Protection**
- **Staff Social Media**
- **School Social Media**
- **Personal Property and Insurance**

Legislation

- Education and Training Act 2020
- Harmful Digital Communications Act 2015
- Privacy Act 2020
- Crimes Act 1961
- Films, Videos, and Publications Classification Act 1993
- Defamation Act 1992
- Human Rights Act
- Harassment Act

Resources

- Netsafe:
 - [Helpline services](#) 
 - [Responding to digital incidents](#) 
 - [Incident support](#) 
 - [How to record digital evidence](#) 
- Ministry of Education | Te Tāhuhu o te Mātauranga: [Digital Technology: Safe and responsible use in schools](#) 
- Ministry of Justice: [Safe harbour provisions](#) 

Release history: [Term 4 2025](#), [Term 1 2023](#), [Term 2 2020](#)

| | |
|--------------------|-------------|
| Last review | Term 4 2022 |
| Topic type | Core |