


Napier Boys' High School

Privacy Policy

Napier Boys' High School complies with the requirements of the Privacy Act 2020. We look after the privacy of everyone associated with our school. In particular, we acknowledge that children and young people are vulnerable and are given particular emphasis in the Act (Principle 4).

We ensure that staff understand our school privacy processes, especially in relation to how we manage personal information, and our process for reporting breaches. Staff are made aware of these processes as needed (e.g. through staff induction and professional development, during staff meetings, and after incidents).

Privacy principles

Napier Boys' High School follows the information privacy principles of the Privacy Act 2020. See [Privacy Act 2020 and the Privacy Principles](#)  (Privacy Commissioner).

- We collect, protect, access, and correct personal information according to the information privacy principles of the Privacy Act. See [Personal Information](#).
- We only use information for the purposes it was collected, except in certain circumstances (e.g. for statistical purposes where the person's identity is not disclosed).
- We are guided by the following policies when we share information:
 - [Sharing Student Personal Information with Parents/Guardians](#)
 - [Sharing Personal Information with External Agencies](#)
 - [Public Sharing of Personal Information](#).
- We only keep information for as long as it is needed and destroy any documents that contain personal information in accordance with the Public Records Act 2005. See [School Records Retention and Disposal](#).

Privacy officer

Under the Privacy Act, we are required to have a privacy officer. Our privacy officer is the headmaster. Their responsibilities include:

- responding to general questions about privacy at our school
- managing requests for personal information
- managing complaints about privacy
- liaising with the Privacy Commissioner in investigations, if required
- informing our school community of serious privacy breaches or risks to the security of personal information the school holds.

Privacy breaches

We follow the Privacy Commissioner's steps for responding to privacy breaches:

1. **Contain**

The school acts to contain the breach. We inform our privacy officer as soon as possible if our school (or an individual at our school) intentionally or accidentally provides unauthorised access to personal information, or discloses, alters, loses, or destroys someone's personal information.

2. **Assess**

We consider each incident on a case-by-case basis to assess the impact and seriousness of the breach.

3. **Notify**

- We decide whether to notify any affected people, and if the breach needs to be reported to the board. If there is no risk of harm, it may not be necessary to notify affected people of a breach.
- If the privacy breach has caused or is likely to cause serious harm (e.g. physical, psychological, emotional, or financial), our privacy officer notifies the Office of the Privacy Commissioner within 72 hours of being made aware of the breach. We also notify the person or people involved and the board.
- We notify NCSC if the breach is due to a cyberattack, or a flaw in a product or online service that our school uses.
- We may notify other third parties (e.g. police, insurers) if necessary.

4. **Prevent**

We investigate the incident and take steps to prevent it from happening again.

See **Breach Management**  (Privacy Commissioner).