École Française Internationale Auckland

Next review: Term 4 2027

Computer Security and Cybersecurity

At schoolshort, we manage our school digital, physical, and information assets in a way that is financially responsible and protects personal privacy (Education and Training Act 2020, Privacy Act 2020). We aim to create a secure and safe online school environment and use a range of cybersecurity practices that are appropriate to the needs of our school to protect IT infrastructure, data, and digital resources from unauthorised access (e.g. suspicious or criminal activity). This may include implementing access security measures, firewall software, back up strategies, regular system updates and maintenance. We also use a secure and safe internet connection and take measures to safeguard school networks.

The principal and board are responsible for school computer security and cybersecurity and reviewing our procedures at least annually. Staff using school devices (e.g. staff laptops) are expected to take appropriate care of their devices, including storing them securely and maintaining digital security measures.

Access security

We aim to use the **principle of least privilege** to ensure that access to school accounts is specific to each person's role and responsibilities. We restrict access to personal information or sensitive data (e.g. limiting access to staff who require it as part of their duties, ensuring discussions of sensitive information are confidential). See **Personal Information**.

All school devices and accounts are password protected and we expect school community members to create, use, and manage passwords securely and keep them confidential.

If staff have a concern that their password has been compromised, they should:

- attempt to reset the password
- report the concern, if appropriate, to relevant staff (e.g. principal, IT support) who may follow responding to digital incidents policy as needed
- contact relevant agencies if needed (e.g. school banking provider, Office of the Privacy Commissioner).

We are guided by **Ministry of Education recommendations** to implement our access security measures.

Remote access to the school cloud service should only be made over trusted wifi networks (using home networks as opposed to public networks). Accessing the school cloud service from home or using a privacy screen in public reduces the risk of access by an unauthorised audience.

Data protection

We aim to maintain the integrity and confidentiality of school information. We regularly back up critical data needed for the day-to-day operations of our school. Back up data is stored in a different location to original data and can be used if something happens to the original (e.g.

lost devices, stolen information). This reduces the risk of data loss and helps us to quickly recover information.

We store data for an appropriate length of time. See **School Records Retention and Disposal**.

We are guided by **Ministry of Education recommendations** for backing up important school data.

Software security

We take a number of measures to ensure school software settings are managed effectively, including:

- setting up software permissions and email security settings appropriately
- updating our permissions and settings as needed
- monitoring alerts and taking any necessary actions.

We are guided by **Ministry of Education recommendations** for configuring security settings.

Upgrades and maintenance

Our school property plan contains a budget for maintaining the digital network, including plans for any required cabling repairs, and replacement of network switches and/or wireless equipment.

Also see **Property Management** and **Property Maintenance and Repairs**.

Managing computer and cybersecurity incidents

Staff, students, and our school community are encouraged to keep alert for cybersecurity concerns and breaches (e.g. checking sender details, acting with caution if emails contain attachments). In the event an incident occurs, we act immediately to minimise distress and harm, safeguard the safety and wellbeing of those affected, and resolve the matter as soon as possible.

- If there is reason to believe school systems may be at risk (e.g. phishing, virus, unauthorised access), we respond appropriately (e.g. reset account logins, scan for viruses/malware, alert our IT provider).
- If École Française Internationale Auckland experiences a cyberattack, we contact relevant agencies for advice and support, as appropriate.
- If there is data breach that impacts personal privacy, we follow the Privacy Commissioner's steps for responding to privacy breaches – see **Privacy Policy**.

Supporting policies

At École Française Internationale Auckland, we have other policies that support our approach to computer security and cybersecurity:

- **Digital Technology and Online Safety**
- **School Social Media**
- **Staff Social Media**
- **Privacy Policy**
- **Responding to Digital Incidents**
- **Asset Management**

Legislation

- Education and Training Act 2020
- Privacy Act 2020

Resources

- Ministry of Education | Te Tāhuhu o te Mātauranga: **Digital technology**

Release history: **Term 3 2025**, **Term 4 2022**, **Term 2 2021**

Last review	Term 4 2024
Topic type	Customised