Global Leadership
Institute
SET YOUR GAZE HIGHER

Online Safety and Security

It is important to stay safe online! Online safety is for all students and staff. Throughout orientation Global Leadership Institute (GLI) students will learn about online safety and safe computing practices which include:

- Managing security settings
- Using software to protect private information
- Physical actions with regards to the devises used.

Tips to stay safe online:

- When creating passwords, it is safest to use unique passwords.
- Never share passwords with anyone.
- Make sure you think before you click! Most cyber attacks start with an email. If students are not sure if an email is safe, then do not click on it. Clicking a dodgy or unsafe link are common ways of being hacked.
- Back up your data! This can be done by USB, Hard drives, the Cloud, and other online storage options. If students are targeted by an attack their files are at risk. Having the files backed up means students will not lose important files.
- Keep your laptops, smart tables and smart phones updated. Many cyber attacks target old devices that do not have updated protection software.
- Be careful about Wi-Fi, GLI has free safe Wi-Fi available for students. Often hackers gain access to devices through unsafe Wi-Fi.
- Keep personal information private.
- Minimise the risk of inappropriate contact using GLI email addresses, report unauthorised communication, and block unknown email addresses.
- Be careful what you share on social media. Hackers use social media too!

What is Cybersecurity?

Cybersecurity is simply a general term for technologies, practices and processes used to protect online data from unauthorized access or misuse. Every day, people play a part in cybersecurity when they follow internet safety tips and cybersecurity best practices.

Cybersecurity words to know:

- Data Breach – A data breach is an incident that results in personal and confidential data being shared.
- Malware – Malware is malicious software intended to disable or infect a devise's functionality.
- Back-ups – Backing up means saving a copy of data on separate storage devices.

Protect your online identity.

You are in charge of protecting your online identity. See the three types of online scams to avoid:

- Online dating scams: Online romance scammers manipulate their victims by forming an intimate personal connection and then using the relationship to gain access to personal and financial information.
- Social media scams: Online scammers are always coming up with new ways to manipulate people on the internet. Look out for social media scams including fake profiles, catfishing, gossip, and click bait.
- Text message scams: Text message scams can be a combination of various online scams, including phishing links. Government entities, banks and legitimate companies will never ask for personal or financial information in a text message.

Report an online scam

To report an online scam please see **ReportCyber** at the Australian Cyber Security Centre

GLI policies

For more information on GLI's policies regarding online safety and security, please see:

Code of Conduct Policy

Health, Safety, and Wellbeing Policy

Security and Safety Policy