LEARNING OUTCOMES

CYBERSECURITY FUNDAMENTALS

Recognise that there are serious security and safety issues associated with the online world and the use of digital technologies.

Recognise the scope of security and safety issues currently associated with the online world, including threats to critical infrastructure and the digital economy.

Recognise that there are strategies for being secure and responsible online, just as there are for being in the real world.

Identify appropriate cybersecurity and cybersafety strategies for online activities.

Talk with teachers, parents and carers, and peers about threats to cybersecurity and cybersafety, including ways to secure home computers and other internet devices.

Choose to be caring about the consequences of decisions in the online world.

Recognise that cybersecurity and cybersafety is a matter for all ICT users.

Choose strategies that secure data and devices, including wireless networks.

Recognise that the language of cybersecurity and cybersafety is specialised and constantly evolving as new threats emerge.

Choose to report cybersecurity and cybersafety concerns such as those arising from online scams, offensive (including prohibited) content, cyberbullying, or the improper use of social networking sites.

MALWARE

Identify common ways that malware can impact.

Recognise that computers can be infected by an email attachment, a bad link in a popup or on a website or social networking site, a bad download, or through an infected USB (flash) drive, CD-ROM or DVD.

OWNERSHIP

Recognise that web content belongs to people, usually by the creator of the work, and that copyright restrictions can apply online.

PRIVACY

Distinguish between concepts of 'public' and 'private' as they apply in the online world. Recognise that protecting identity is part of cybersecurity.

Choose cybersafe and secure strategies for social networking and online gaming: adjusting privacy set- tings to friends only, placing limits on personal information about self and others, respecting right to privacy, observing netiquette, and reporting improper use.

Recognise that personal information can be text and images.

POSTING

Interpret how information might be used online, and recognise where information can go online. Recognise that posted content remains online forever. Describe the meaning of a 'digital footprint'. Identify features of cyberbullying, and recognise that it can have serious consequences.

SCAMS

Recognise that some people go online with the intent to commit theft, fraud or vandalism.

Identify key features of online scams, including spam, phishing attacks, auction and shopping scams, and social engineering.

SHARING

Recognise the risks associated with file-sharing, such as malware infection, illegal (copyrighted) content, and prohibited content.

Identify key features of secure and safe file-sharing, posting and downloading.

TRANSACTING

Recognise universally-accepted signs of security for online transacting and providing personal information, including https, the locked padlock icon, and digital certificate.

TRUTH

Recognise that web content can be wrong, biased or out-of-date.