Cybersafety in Schools Overview

Sections

A. The Changing Cybersafety Landscape
B. Digital Citizenship and the New Zealand Curriculum
C. The LEARN: GUIDE: PROTECT: Framework

A. The Changing Cybersafety Landscape

In the past decade there have been significant changes to technology and the way it is used in New Zealand schools. This has presented new challenges for educators in creating an environment where teachers and students are confident in the safe and secure use of technologies. With the upcoming introduction of ultra-fast broadband in New Zealand, schools will increasingly face a more complex technical environment that demands an appropriate approach to cybersafety.

Previous models of school cybersafety relied on teachers and administrators preventing access to specific content. Most New Zealand schools have established ICT guidelines and procedures, both technical and managerial but new uses of technology requires the focus of cybersafety to expand beyond policies and procedures to include discussion, action, and teachable moments in the classroom.

Ongoing staff and student education programmes are fundamental to keep pace with changing technology use in schools. Students need to build skills and knowledge to effectively manage challenge in cyberspace themselves. Educators need to increase their capability to guide young people in building their own cyber safety skils.

The concept of creating a cyber safe environment has moved from *protecting* people and to giving people the *skills, knowledge and confidence* to maximise the opportunities the effective use of technology can bring.

When a young child enters school, they will have limited practical cyber safety skills. By the time they graduate, we expect them to be ready to fully participate in a digital society. In the intervening years they will ***learn*** cyber safety skills with the assistance of a ***guide***, against a backdrop of reducing levels of ***protect***ion.

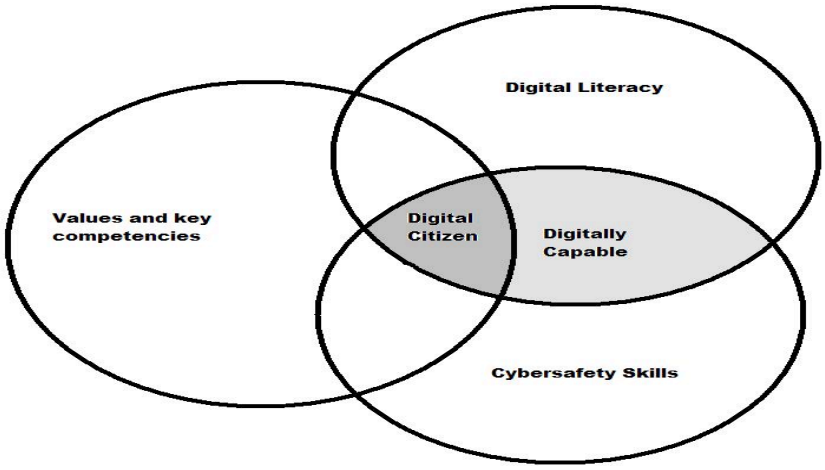
B. Digital Citizenship and the New Zealand Curriculum

Drawing from the Key Competencies and Values in the NZ Curriculum and a growing body of research knowledge, NetSafe, in consultation with New Zealand teachers has produced this definition of a New Zealand Digital Citizen.

A digital citizen:

- is a **confident and capable** user of ICT
- uses technologies to **participate** in educational, cultural, and economic activities
- uses and develops critical **thinking** skills in cyberspace
- is literate in the **language, symbols, and texts** of digital technologies
- is aware of ICT **challenges** and can **manage** them effectively
- uses ICT to **relate to others** in positive, meaningful ways
- demonstrates honesty and **integrity** and **ethical behaviour** in their use of ICT
- **respects** the concepts of privacy and freedom of speech in a digital world
- **contributes** and actively **promotes the values** of digital citizenship

Digital literacy or the ability to understand and fully participate in the digital world is fundamental to digital citizenship. It is the combination of technical and social skills that enable a person to be successful and safe in the information age. Like literacy and numeracy initiatives which provide people with the skills to participate in the work force, digital literacy has become an essential skill to be a confident, connected, and actively involved life long learner.



THE LEARN: GUIDE: PROTECT: FRAMEWORK

learn
guide
protect

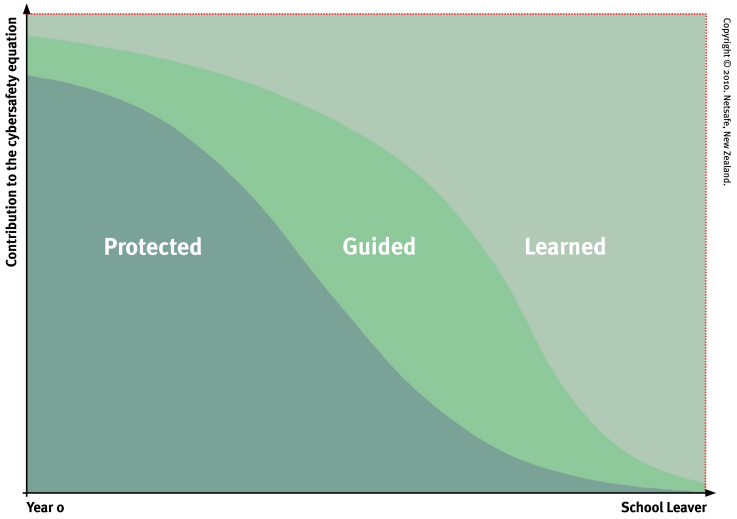
In response to the changing requirements of schools, NetSafe has developed a new model of cybersafety called Learn:Guide:Protect: (LGP). The LGP model allows educators to create a student-centred learning pathway from a protected environment through to a self-managing state. The model recognises growing teacher expertise and acts as a central hub of information and knowledge about effective cyber safety practices contributed by teachers.

LGP is divided into three components: the skills students **learn** to keep themselves safe, the **guidance** they access to learn how to manage challenges, and the **protective** mechanisms schools can use to improve their immediate safety..

1. Learn: Educating students to develop positive, ethical behaviours in cyberspace

2. Guide: Professional learning resources and lesson activities for educators to teach digital citizenry and to create a positive school culture of digital citizenship.

3. Protect: Technology, infrastructure, and school developed policy that supports the establishment of a safe and secure technology environment.



The diagram shows the changing emphasis of the three components of the framework as students progress through school.

In the early school years, the protective measures are of critical importance so that young students can safely explore a wide range of online experiences. Teacher guidance will provide appropriate learning opportunities to lay the foundation for cyber safety skills

As the students go through the intermediate/ early secondary years, the effectiveness of protective measures drops off markedly, even when protection measures are in place. Through this middle period of schooling, more adult guidance is required to bridge the gap between students' skills and the diminishing effectiveness of protection systems.

At upper secondary levels, students require regular opportunities to develop self-management skills to prepare them for active participation in a digital society as school leavers.

LEARN: Opportunities for Students

The learning pathway for digital citizenship and cyber safety follows the New Zealand Curriculum's learning pathways. At the core of student learning is a digital citizenry curriculum that provides opportunities to build upon existing skills. The objective of a successful digital citizenship education is to develop school leavers who are capable of managing their own online safety.

Learning in Years 1-6: Focus on building a range of digital literacy skills

A successful cyber safety programme at this stage focuses on students developing skills through experiences where they have both reasonable protection and adult guidance. This stage lays the groundwork for key competencies and values young people require to effectively utilise digital technologies. Students are likely to be using a range of technologies often with specific instructions and close monitoring by adults.

Learning in Years 7-10: Focus on competencies, values and behaviours

A successful cyber safety programme at this stage needs to be responsive to the growing independence and social awareness of young people as they explore more complex online contexts, sometimes without adult supervision. This stage places a stronger emphasis on adult guidance and authentic learning experiences to increase student self-sufficiency. Integrating key competencies and values into cyber safety education to build on students' existing skills is vital. During these years administrators are likely to be assessing the appropriate balance between providing authentic online learning opportunities and students' exposure to risk.

Learning in Years 11-13: Focus on opportunities to practice skills in an authentic context

A successful cyber safety programme at this stage will allow students greater opportunities to practice digital citizenry skills. It should recognise the diverse abilities, aspirations and growing responsibility of senior students. It should also recognise that personal values and key competencies have gained significance for these young people as they develop the capabilities they will need as adults in a digital society. Educators need to provide students with regular opportunities to critically analyse their own values and actions in cyberspace.

GUIDE: The Teacher's Role in Cybersafety

The shift from protecting students from inappropriate material to providing opportunities where students can learn to self manage their activity, changes the emphasis of responsibility for a school cyber safety programme. It places more responsibility on classroom teachers who support young people as they use technology in learning activities. Young people want

opportunities to discuss online challenges with respected and authoritative adults. This does not require teachers to be technology experts, but it is important that their knowledge is broad, authentic and current.
Developing teacher capability so they can act as effective cyber safety guides is vital.

PROTECT: Shaping the environment

The protection component consists of policies, practices and services designed to create a safer space. These include filtering, security, and monitoring solutions. Filtering makes an important contribution to a safe environment particularly for very young people. Some protective measures, like filtering however, become less effective as a cyber safety tool as students mature. This creates both the opportunity and the need for learners to build personal cyber safety skills and knowledge. Schools will continuously assess the risks and benefits of protective measures.

Additional support for establishing secure networks in schools is provided by the Ministry of Education. Visit: http://ict-helpdesk.tki.org.nz/News