
Key DER-NSW domains and themes of digital citizenship

Educators around the world are finding it useful to define the key components of good digital citizenship to help students better navigate their online lives. The Digital Education Revolution – NSW has developed a set of digital citizenship domains upon which to base a digital citizenship education program. Support materials for teaching digital citizenship are being progressively developed as part of the Digital Education Revolution – NSW. They will include teacher professional learning and parent information.

The NSW Digital Citizenship strategy reflects a worldwide movement to address and characterise digital citizenship, which makes it imperative to address this in Australian schools. The direction taken in the UK has been towards encouraging young people to see online environments as communities they are helping to shape, so that they will act more responsibly. Digizen.org in the UK states on its website under the heading: What makes you such a good digizen?

Digital citizenship isn't just about recognising and dealing with online hazards. It's about building safe spaces and communities, understanding how to manage personal information, and about being internet savvy—using your online presence to grow and shape your world in a safe, creative way, and inspiring others to do the same.

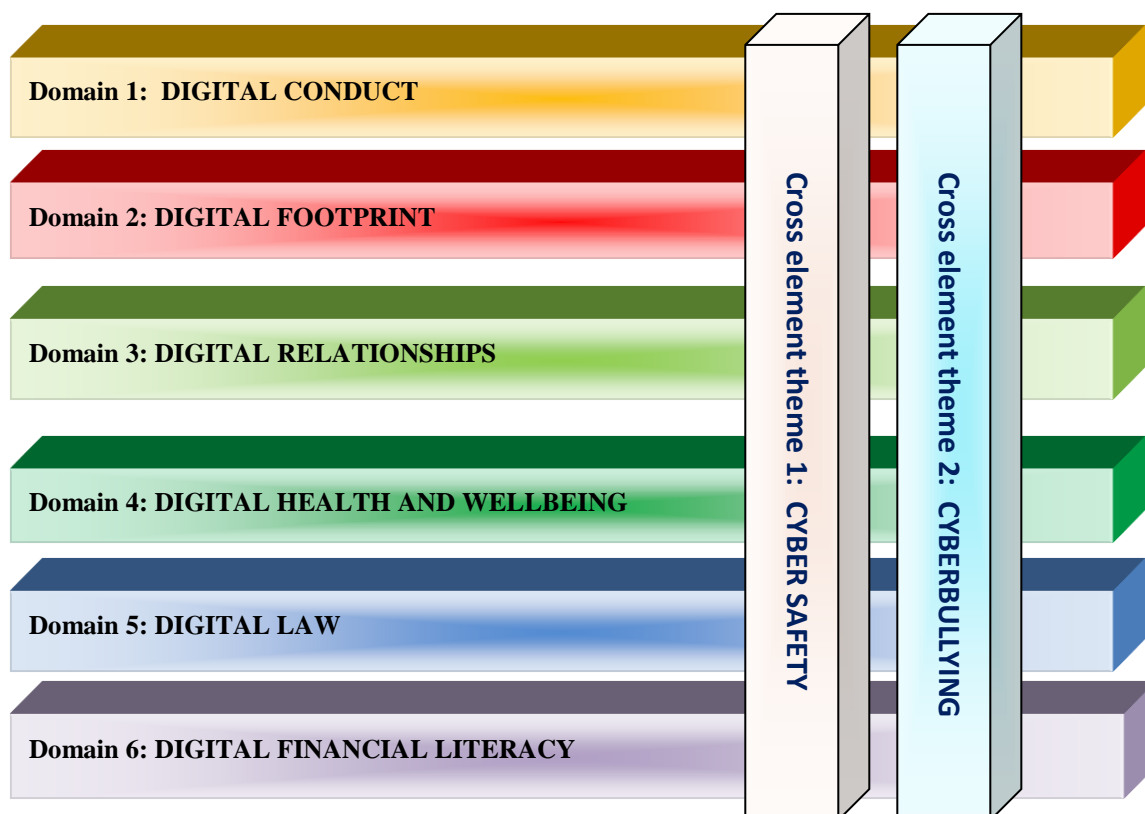
In the US the focus has been on individual ethical behaviour. United States educator and author Mike Ribble has developed nine themes of digital citizenship, defining it as:

appropriate, responsible behaviour with regard to technology use and asks in regard to how this should be taught: 'If not here (schools) , where? If not now, when? If not you, who?'

National resources have been developed in Australia and elsewhere to address cyber bullying and assist with digital safety and intellectual property. These include Budd:e from the Department of Broadband, Communication and the Digital Economy; cyber(smart:) from the Australian Communications and Media Authority (ACMA) and Think You Know from the Australian Federal Police and Microsoft Australia. These will be utilised as sources and references. The focus is on young people as stakeholders in positive internet use.

Key components of digital citizenship

The NSW Digital Citizenship model has six key elements with two interwoven themes:



1 Digital conduct

This domain includes one's responsibilities and rights in an online world, and the concepts of ethical, responsible and respectful online use. It includes positive online conduct, codes of practice, 'netspeak' and 'netiquette', interacting properly with online contacts, courteous email forwarding and thinking before posting. It includes knowledge of how to deal with inappropriate advertising and pop-ups, what to do when seeing things you wish you hadn't and how to report online security concerns.

Students need to be able to recognise inappropriate or suspicious behaviour online and know how to report it. The domain also looks at the responsibility of protecting internet-connected computers, privacy and safe practices when sharing information online. The focus is on how ICT can be used to enhance interpersonal relationships and to introduce students to a new collective responsibility: the values of a good digital citizen, how to be one, and the idea that online environments are communities that users are helping to shape for the future.

2 Digital footprint

This domain includes understanding of the trail left by activity in a digital environment, recognising that nothing in the online world is confidential and understanding that what is online about us can last for years. It includes considering what a future employer may see and how information could be used by businesses or criminals. It includes thinking about potential consequences before posting and tagging of photos and videos or blogging, considerations when using a webcam, identifying inappropriate or offensive content and understanding how things can be used online.

Students are asked to be positive creators as well as users of online content and to understand the benefits of collaborative, social learning using online tools, and pooling or sharing knowledge, resources, reflections, brainstorming etc. The domain focuses on balancing the desire for a public presence with the need to protect personal information. It also focuses on building a positive online reputation while experiencing a wide range of online communication experiences and the sense of satisfaction and excitement that comes from feeling part of a global online community.

3 Digital relationships

This domain looks at new social norms in networked public cultures, online friends, privacy settings and identity protection. It includes when and how to restrict access or limit personal information about self and others, as well as selecting photos and developing appropriate online profiles that do not reveal too much, and the right of others to privacy. It includes recognition of the risks of social networking, that there is no guarantee that a person online is who they say they are, recognising grooming or luring tactics, cyber stalking, unwanted contact and how to report abuse. It also addresses use of avatars, virtual worlds and chat rooms, the responsibility to protect others from humiliation, and how to deal with words or photos that may hurt others.

Students should know how to change privacy settings, how to block people who are being inappropriate and how to report abuse online. They should understand that caching and the ability to store and forward means there is no such thing as delete in an online world. The main focus is how to have fun while social networking, while understanding the risks and using the technology safely and responsibly.

4 Digital health and wellbeing

This domain looks at balance and lifestyle, and balancing time online with relationships with friends and family in the real world. It also includes occupational health and safety issues such as eye strain, care for neck, shoulders and back and ergonomic advice. Gaming is part of this topic: having fun competing against and chatting with people from all over the world but being in control, selecting no-risk identities and being aware of risks such as

desensitisation to violence, addiction and bullying through abuse of other players. It includes awareness of grooming or luring via online gaming and what to do if something makes the student feel uncomfortable online. The main focus is the awareness of problematic computer use, caring for one's physical and mental wellbeing and having a balanced lifestyle.

5 Digital law

This domain includes understanding ethical responsibilities when using content developed by others, intellectual property right, and how to avoid plagiarism and acknowledge and reference sources. It includes secure and legal P2P/filesharing, legal and illegal access to music, movies and television shows, and the dangers of creating viruses, forwarding spam and the risks of hacking, as well as being alert to computer-connected scams and unethical marketing. The focus is on the productive use of online resources for both study and entertainment, while understanding the potential consequences of illegal actions such as plagiarism by downloading for themselves and others.

6 Digital financial literacy

This domain includes how to be an aware consumer in the digital economy. It looks at shopping online, identity protection, financial security, understanding online fraud and identifying phoney or insecure websites, as well as phishing and other scams that attempt to defraud money or to steal personal details (identity theft). It also includes online gambling and other games that cost. The focus is on taking advantage of the convenient services online while protecting oneself, one's family and one's computer.

Cross domain themes

1 Cybersafety

This theme runs across each domain; it covers the concept that cyber security and personal online safety precautions are the responsibility of every computer user and that all users should have a personalised safety and security action plan.

2 Cyberbullying

This theme runs across each domain; it promotes the expectation that all students should be active in preventing cyberbullying and understand that even one-off hostile cyber actions can have a widespread negative impact, due to the rapid dissemination and relative permanency of the message sent. Students should understand the characteristics and forms of cyberbullying and hostile cyber behaviour, and the steps they can take if experiencing or observing these behaviours.