Digital Education Revolution - NSW

Digital Citizenship

*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.* - Digizen (1)

In 2010 in NSW support materials for teaching Digital Citizenship and Digital Safety have been developed for years 7-10 as part of the Digital Education Revolution - NSW. This includes:

1. Year 10 - Term 4 2010 series of lessons Digital Citizenship with focus on social networking issues. These include virtual activities and interaction with existing quizzes and resources and are a blend of face to face and online activities so that teachers engage with the content.
2. Teacher professional learning with focus on social networking and online issues
3. Parent education program on digital citizenship with focus on social networking – virtual activities
4. Years K-10 developmental program

For 2010 the priority is Year 10 with a focus on issues relating to social networking. It is intended that these materials will be taught to year 10 in Term 4, 2010, and that by the end of 2011 schools will be able to implement a 7-10 digital citizenship program.

**Background**

The focus in 2009 was on use of the laptops, the software and on development of technology and digital learning skills. It is now time for a set of common understandings about learning and working in digital environments.

Many users do not know what constitutes appropriate technology use and both students as well as adults misuse and abuse technology. While acceptable usage policies and user charters are important, they are not enough. Students need to understand what is appropriate and inappropriate and this will require education about the appropriate use of technology.

Digital Citizenship is a way to teach students what it means to be a good digital citizen and how to go about being one. Being a good citizen includes anything from following certain email protocols to paying for proprietary content online and engaging in constructive online dialogue.

There is an emerging worldwide movement to address and characterise digital citizenship which makes it imperative that this is addressed in Australian schools.
**Social Networking**

In NSW, social networking sites are becoming part of everyday life, woven into the social fabric of students and increasingly teachers. Society is increasingly relying on social networking to connect, collaborate and learn. Social networking online are friendship-driven practices. This means youth are almost always associating with people they already know in their offline lives. The majority use this new media to ‘hang out’ and extend existing friendships through these social networking sites. Such interactions are now fixtures of youth culture and teen social life. For them participation in the digital age means more than being able to access ‘serious’ online information.

Schools have a role in educating students on the safe and responsible behaviours to adopt when using social networking services and other forms of new technologies as part of their general digital literacy education.

The focus in Year 10 will be on issues relating to social networking in the light of Minister’s announcement that there may be access to social networking sites off DET premises for senior students. A limited trial is planned in 5 schools in Term 4.

**Use of Australian resources**

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 (2); *CYBER(SMART:)* from the Australian Communications and Media Authority (ACMA) (3) and *Think You Know* from the Australian Federal Police and Microsoft Australia (4). NSW DET Curriculum Directorate through CK-12 and CLI are requested to utilise these as sources and references where relevant when preparing work units. ACMA materials will be valuable and are creative commons.

**Cyberbullying and Cybersafety**

There are the two cross domain themes. The Alannah and Madeline Foundation’s Cybersafety and Wellbeing Initiative, ACMA and Budd:e materials contain much on Cybersafety while ACMA also has a Cyberbullying focus. Note that Digital Citizenship is wider than a cyber bullying or cyber safety program though these themes will be referred to where appropriate.

**Focus**

The focus, while highlighting risks, is on young people as stakeholders in positive internet use.
The six key domains with two interwoven themes for the 7-10 Digital Citizenship program are as follows:

- **Domain 1: DIGITAL CONDUCT**
- **Domain 2: DIGITAL FOOTPRINT**
- **Domain 3: DIGITAL RELATIONSHIPS**
- **Domain 4: DIGITAL HEALTH AND WELLBEING**
- **Domain 5: DIGITAL LAW**
- **Domain 6: DIGITAL FINANCIAL LITERACY**

**Cross domain theme 1: CYBER SAFETY**

**Cross domain theme 2: CYBERBULLYING**
THE DOMAINS OF DIGITAL CITIZENSHIP

1. **Digital Conduct**
The focus of this domain 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. Content includes:

i. Responsibilities and rights in an online world
ii. The concepts of ethical, responsible and respectful online use.
iii. Positive online conduct and codes of practice
iv. ‘Netspeak’ and ‘netiquette’ interacting properly with online contacts e.g. courteous email forwarding and thinking before posting.
v. How to deal with inappropriate advertising and pop-ups
vi. What to do when seeing things you wish you hadn’t
vii. How to report online security concerns
viii. Recognising inappropriate or suspicious behaviour on line and know how to report it.
ix. Protecting internet connected computers, privacy and safe practices when sharing information online.

2. **Digital Footprint**
The focus of this domain is on balancing the desire for a public presence with the need to protect personal information. It also focuses on the building of a positive online reputation while experiencing a breadth of online communication experiences and the sense of satisfaction and excitement from feeling part of a global online community. Content includes:

i. Understanding of the trail left by activity in a digital environment
ii. Recognising that nothing in the online world is confidential and understanding that what is online about us can last for years e.g., considering what a future employer may see or how information could be used by businesses or criminals.
iii. Thinking about potential consequences before posting and tagging of photos and videos or blogging and understanding how things can be used online.
iv. Considerations when using a webcam
v. Identifying inappropriate or offensive content
vi. Microblogging e.g. Twitter
vii. Being a positive creator as well as user of online content
viii. Understand the idea of collaborative, social learning using online tools and pooling / sharing knowledge, resources, reflections, brainstorming etc for positive ends.

3. **Digital Relationships**
The main focus of this domain is how to have fun while social networking, connecting to friends and families yet to understand the risks and use them safely and responsibly. Content includes:

i. New social norms in networked public cultures
ii. Online friends
iii. Privacy settings and identity protection. When and how to restrict access or limit personal information about self and others.
iv. How to block people who are being inappropriate and how to report abuse online.
v. Selecting photos and developing appropriate online profiles that do not reveal too much. Understanding that caching and the ability to store and forward means there is no such thing as delete in an online world.
vi. 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.
vii. Use of avatars, virtual worlds, chat rooms
viii. The right of others to privacy. The responsibility to protecting others from humiliation and how to deal with words or photos that may hurt others.

4. Digital Health and Wellbeing
The main focus of this domain is the awareness of problematic computer use, caring for one’s physical and mental wellbeing and having a balanced lifestyle.
Content includes:
i. Balance and lifestyle - balancing time on line with relationships with friends and family in the real world.
ii. Occupational health and safety issues such as eye strain, care for neck, shoulders and back and ergonomic advice.
iii. Gaming - 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.
iv. Awareness of grooming or luring via online gaming and what to do if something makes them feel uncomfortable online.

5. Digital Law
The focus of this domain is on productive use of online resources for both study and entertainment while understanding the potential consequences of illegal actions, download and plagiarism for others and themselves.
Content includes:
i. Understanding ethical responsibilities when using content developed by others,
ii. Intellectual property,
iii. How to avoid plagiarism and how to acknowledge and reference sources
iv. Secure and legal P2P/filesharhing,
v. Legal and illegal access to music, movies and television shows
vi. Dangers of creating viruses, forwarding spam and risks of hacking
vii. Being alert to computer connected scams and unethical marketing.

6. Digital Financial Literacy
The focus of this domain is on taking advantage of the convenient services online while protecting oneself, one’s family and one’s computer.
Content includes:
i. How to be an aware consumer in the digital economy.
ii. Shopping online, identity protection and financial security,
iii. Understanding online fraud and identifying phoney or insecure websites as well as phishing and other scams that attempt to defraud of money or attempt to steal personal details (identity theft).
iv. Online gambling and other games that cost.
Cross domain themes

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

References:

5. ACMA Internet Safety and Security Guidelines from Peer and Personal Safety – Managing Online Safety p.14 [http://www.cybersmart.gov.au/Schools/Teacher%20resources/Middle%20secondary/~/media/Files/Teacher%20resources/Middle%20secondary/ACMA_MidSec_ManagingOnlineSafety.ashx](http://www.cybersmart.gov.au/Schools/Teacher%20resources/Middle%20secondary/~/media/Files/Teacher%20resources/Middle%20secondary/ACMA_MidSec_ManagingOnlineSafety.ashx)