Activity 1: Your online presence

- **Activity overview:**
  This activity requires students to Google their own name to determine their online presence and evaluate their online reputation. They can also reflect on how to protect their online reputation by editing and deleting items that are attached to their online profiles. Having established these steps, students are encouraged to go home and review and edit their online profiles.

- **Activity outcomes:**
  - Identify and describe online activity.
  - Understand that a person’s use of digital technology and online activity is revealing of their personal characteristics.
  - Identify and describe online presence and reputation.
  - Identify how individuals can protect their online reputation.
  - Evaluate and edit online profiles.

- **Activity duration:** Tasks A, B and C can be completed in class in 60 – 75 minutes. The final part of Task C will need be explained in class, so that students can complete the review of their online user profiles at home. Teachers may like to use their own online presence as an example to guide students through the questions and enable them to develop steps to protect their online reputation. Teachers are also encouraged to revisit this activity after students have had the opportunity to edit their online profile.

- **Terminology used in this activity:**
  - Online: Being online means being connected to the internet.
  - Reputation: The opinion that we have about someone or something.
  - Profile: A visual display of personal data associated with a specific user, for example their name, age, gender, etc.

Activity 2: Online Security

- **Activity overview:**
  This activity requires students to think about how safe and secure they are online as they discuss and learn about secure networks, secure sites, privacy settings and passwords. Students can use this information to determine if their Wi-Fi network at home is secure and protected by a strong password.

- **Activity outcomes:**
  - Understand how to be safe and secure online.
  - Determine what makes a secure network.
  - Identify signals of a secure website.
  - Identify the differences between weak and strong passwords.
  - Understand what constitutes a strong password.

- **Activity duration:** 60 – 75 minutes. The final part of Task A will need be explained in class, so that students can review their Wi-Fi password at home.

- **Terminology used in this activity:**
  - Online security: Being secure and safe while online.
  - Secure networks: Networks that are protected by a strong password so that others are not able to access or intercept.
  - Secure sites: The connection between the user and the website is encrypted.
  - Privacy Settings: A series of settings that enable you to protect your privacy such as a password.
  - Passwords: A password is used to gain access to areas on the Internet where you may wish to protect or restrict access to personal information.
  - Hacked: When someone accesses your account using a script or code to bypass the usual security measures and accesses your private information.
Activity Sheets Teacher Introduction

Activity 4: The online you

Activity overview:
This activity requires students to reflect on their online activity and whether they are consumers or creators or a combination of both. Students also have the opportunity to explore what is good behavior online and what constitutes antisocial behaviour.

Activity outcomes:
- Identify the qualities of a good digital citizen.
- Recognise the importance of appropriate and responsible use of digital technology.
- Recognise the importance of respectful and responsible online behaviour.

Activity duration: 60 – 75 minutes.

Terminology used in this activity:
Consume: The way that people interact with online content. For example, they view videos, listen to music, retweet, regram and repost.
Create: Production of original material that is posted online.
Etiquette: A set of rules that define polite behaviour in a social situation.
Antisocial Behaviour: Behaviour that is disrespectful to others and the laws and customs of society.
Cyber bullying: When technology is used to deliberately and repeatedly engage in hostile behaviour in order to harm someone.
Cyber harassment: When technology is used as the tool to harass another person.
Cyber stalking: The repeated use of technology to harass or frighten someone, for example by sending threatening emails.
Trolling: The act of posting inflammatory or off-topic messages in an online community.

Activity 3: Friends and followers

Activity overview:
This activity requires students to think about the friends that they have online, how they are connected, whom they follow and who follows them. They also have the chance to discuss why they follow famous people and why they allow others to follow them.

Activity outcomes:
- Understand how online communication is similar to, but differs from, in-person communication.
- Understand that online activities can have associated risks.
- Think critically about how individuals can protect themselves online.

Activity duration: 60 – 75 minutes.

Terminology used in this activity:
Online friends: Friends who you may never meet in person but who you interact with online via social networks, email, games, etc.
Face-to-face or in-person friends: Friends who you meet in person.
Online chat: Talking online to someone either through text or video and/or audio.
Follow: When you follow someone on a social network and have access to their public posts.
Followers: The people who follow you on social networks and who have access to your public posts.

Cracked: When someone accesses your account because they have figured out your password.
Lacked: When someone accesses your account because your account lacks the protection it requires.
Activity 5: Managing your personal digital devices

Activity overview:
This activity requires students to review how they manage their personal digital devices and in turn determine if this use is appropriate and responsible. The questions and activities require students to describe and evaluate the content that they download, and in doing so identify risks associated with downloads and how to prevent them.

Activity outcomes:
- Identify and describe the use of personal digital devices.
- Think critically about how individuals can protect themselves and their digital devices while online.
- Acknowledge the pros and cons of downloads.

Activity duration: 60 – 75 minutes.

Terminology used in this activity:
Adware: Software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online.
App: An abbreviation for application. An app is a piece of software designed to fulfil a particular purpose. An app is usually downloaded by a user to a mobile device.
Digital device: A digital device is an electronic device that can receive, store, process or send digital information.
Download: To download a file means to transfer it from one computer to another. This can refer to a music file, document or photo, transferred from the Internet to a home or work computer.
Malware: Malware is software which is specifically designed to disrupt or damage a computer system.
Ringtone: A ringtone is a sound made by a mobile phone when an incoming call is received. Phones generally have a number of default ringtones to choose from but consumers are also able to download and install various ringtones to personalise their phones.
Spyware: Software that enables a user to obtain information about another's computer activities by transmitting data without permission from their hard drive.
Trojan: Trojan is a software program that appears legitimate, but performs some illicit activity when it is run. It may be used to locate password information or make the hardware’s operating system more vulnerable or destroy programs or data on the hard disk. A Trojan is similar to a virus.

Worm: A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

Activity 6: In excess

Activity overview:
This activity requires students to examine their online behaviour and consider if they spend too much time online. Students are also asked to investigate the warning signs of too much time spent online and how to change this behaviour. Using this knowledge, students will conduct a debate.

Activity outcomes:
- Describe online behaviour.
- Identify positive and negative online behaviour.
- Determine typical teenage online behaviour.
- Reflect on contemporary society’s dependence on digital technology.

Activity duration: 60 – 75 minutes. More time may be required depending on class size for Task E.
Activity 8: Game Over

Activity overview:
This activity requires students to interview a gamer and determine why people play electronic games. In addition, students are asked to identify the advantages and disadvantages of electronic gameplay, and to determine what limits should be imposed on electronic gameplay. Students are also required to observe a parent or guardian playing an electronic game and discuss their view of electronic games.

Activity outcomes:
- Identify and describe types of electronic games.
- Identify and describe the advantages and disadvantages of electronic gameplay.
- Identify how to stay safe whilst playing electronic games.
- Discuss how adults view electronic games.
- Evaluate individual electronic gameplay.

Activity duration: 60 – 75 minutes. Task E requires students to complete some work at home.

Terminology used in this activity:
Console: A console is a device especially made for electronic gameplay.
Electronic game: An electronic game is a game that employs electronics to create an interactive system with which a player can play.
Gameplay: Gameplay is a term to describe the interactive gaming process.
Hand-held device: A digital device that can be used in the hand.
Platform: The electronic systems used to play electronic games are known as platforms.