

## What do I already know?

- I understand that I have to make choices when using technology and that not everything is true and/or safe.
- I can use technology in ways which minimises risk. e.g. responsible use of online discussions, etc.
- I can create strong passwords and manage them so that they remain strong.
- I can independently, and with regard for e-safety, select and use appropriate communication tools to solve problems by collaborating and communicating with others within and beyond school.
- I can use appropriate strategies for finding, critically evaluating, validating and verifying information.
- I can find *report* and *flag* buttons in commonly used sites and name sources of help
- I can use social networking websites appropriately, keeping an adult informed of my online activity and make good choices when presenting myself online
- I can judge what sort of privacy settings might be relevant to reducing different risks
- I understand my impact on the online world.

## What will I learn?

- I use different passwords for a range of online services. I can describe effective strategies for managing those passwords (e.g. password managers, acronyms, stories). I know what to do if my password is lost or stolen
- I can explain the importance of self-regulating my use of technology; I can demonstrate the strategies I use to do this (e.g. monitoring my time online, avoiding accidents).
- I can demonstrate strategies to enable me to analyse and evaluate the validity of 'facts' and I can explain why using these strategies are important.
- I can describe how to capture bullying content as evidence (e.g screen-grab, URL, profile) to share with others who can help me.
- I can show I understand my responsibilities for the well-being of others in my online social group.

# Year 6 Online Safety



## Vocabulary

Antivirus- a type of software application that identifies and stops a range of online threats by scanning files and applications on your computer

Trojan-Trojan, also called Trojan horse virus, a type of malicious computer software (malware) disguised within legitimate or beneficial programs or files.

Bot, scams-Any type of fraudulent activity conducted online

Phishing-The meaning of PHISHING is the practice of tricking Internet users into revealing personal or confidential information

Location-based settings-A location-based service (LBS) is a software service for mobile device that requires knowledge about where the mobile device is geographically located

Trolling-make a deliberately offensive or provocative online post with the aim of upsetting someone or eliciting an angry response from them:

Sexting-the action or practice of sending sexually explicit photographs or messages via mobile phone:

