VILLAGE: (ages 9-10 years) All Scenarios Summary
Introduction: Rapid Fire Quiz
Exploration of children's online experience and who their trusted adults are. List of quiz questions.
Scenario 1: Digital Footprint
This lesson explores how our digital footprint is created, how it can affect our reputation now, and in the future, both positively and negatively. The concept of good digital citizenship is explored, including the need to protect both their own and other people's digital footprints
Scenario 2: Clickjacking – Sensational headings
Learners are encouraged to recognise Clickbait and to be sceptical of such tactics with an awareness that clicking may infect their device with malware, reveal their personal information or expose them to inappropriate content.
Scenario 3: Webcam Wise
This lesson explores the benefits and risks of webcam communication. Learners are encouraged to recognise the warning signs of a negative relationship and to know how to respond safely to unwanted contact.
Scenario 4: Safe Sharing – Bullying and IP addresses
This introduces Internet Protocol (IP) addresses and the type of information which they contain. Children will explore the differences between on and offline communications, between banter and bullying, and how to reduce the risk of unintentional upset.
Scenario 5: Online Gaming
This lesson explores how people can connect, communicate and collaborate through online gaming. It looks at the temptation to accept "friend" requests. It also addresses the problems of spending too much time gaming and of "griefers" who deliberately upset game play.
Scenario 6: Boundaries *(Includes pre-lesson safeguarding advice)*
This teaches that the same principals apply to online relationships as with face-to face. It allows schools to define the term "rude" and explores why someone might send a rude photo. It looks at how it might make Taff feel, how it could put him at risk and strategies for reducing the risk.
Scenario 7: Illegal Downloads *(includes teacher advice on Copyright)*
This lesson looks at the differences between downloading and streaming. It introduces the concepts of copyright, piracy and the ethics of downloading content from illegitimate sites.
Scenario 8: Downloading Apps
As well as age limits, this scenario explores the different types of permission that apps may request. It looks at the pressures to use games that are for older age groups and explores the risks of doing so.
Scenario 9: Images *(includes pre-lesson advice on Sexting)*
The focus of this lesson is on individual responsibility, an awareness of consequences (including damage to reputation, bullying, emotional distress and illegality) and developing strategies to resist requests for inappropriate behaviour. Children will learn what to do if they make a mistake and how to respond to receipt of inappropriate images.
Scenario 10: Perfect Passwords
This lesson looks at why we need passwords and what could happen if they are shared or stolen, including the risk of hacking and identity theft. Strategies for creating and protecting passwords are addressed alongside what to do if a password has been compromised. An extension exercise looks at 2 factor authentication, Captcha, Biometrics, Password Managers.
End Rapid Fire Quiz
This lesson reviews learning from all scenarios and introduces the final rapid fire quiz.