Gooseberry Parent Advice

1. SAFE SHARING: free Wi-Fi What I should know…

Free, Unsecured Wi-Fi

Wi-Fi hotspots are found in many public areas such as cafes, hotels and airports. Sometimes they are secure and encrypted, requiring a password and login details. Often, they are unsecured and present a serious security risk if users share sensitive information. Users are usually required to login with personal details such as name and email address in order to use public Wi-Fi.

'Https'

Website addresses that begin 'https' rather than 'http' use encryption to protect communications to and from it. But check the address carefully - fraudulent websites may also use 'https'

What do I need to know?

Public Wi-Fi is vulnerable to attack in several ways. Fraudsters may set up a fake Wi-Fi to mimic a genuine one in order to trick users into registering or they may intercept communications between genuine Wi-Fi users and providers. Their aim is to gather information or download malware onto users' devices. It is sensible to avoid un-password protected networks and to avoid "auto-connecting" with WiFi. If you have to share sensitive information, use your mobile phone network and 'https' secure websites instead. If regularly using public Wi-Fi a Virtual Private Network (VPN) can be used, which encrypts all communications. These vary in security levels – some are free and others are paid for – you should research their security and privacy policies before selecting.

What to talk about with your child

- **Discuss** their understanding of public Wi-Fi and the security issues surrounding it. Do they know what encryption is? Explain the risk of hacking and malware.
- **Remind** them not to use un-password protected Wi-Fi networks.
- **Help** them adjust their device settings not to "auto-connect" to Wi-Fi.
- **Remind** them, if they do use public Wi-Fi to restrict activity to web-browsing and not to share or access sensitive information such as login, password or financial details, even on a secured public Wi-Fi. (Keeping separate, strong passwords for different accounts provides protection if one password is compromised).
- **Advise** them that, if using public Wi-Fi, they should log-out as soon as they have finished.
- **Talk** about the pressure to share online and how it is important not to over-share and to resist the urge to share straight away – wait and use a secure home connection.
- **Agree or remind** them of some general rules about what and with whom it is safe to share online.