Online Safety & Cyber Security

This document, which is aimed primarily at staff but can also be used by secondary students, provides some information about online safety and cyber security, as well as a list of resources which can be useful for a range of audiences.

Online Safety

Privacy: Social media is highly prevalent and popular, and, while it can be useful or beneficial, it can also be a way for personal data to be shared with and viewed by others.

- To ensure you don't share any personal data that you don't want to, ensure that your privacy settings are the highest possible (while still allowing you to reasonably use the social media)
- Details such as your date of birth should be kept hidden from everyone, and viewing your profile should be restricted to your friends only (on some sites, such as Facebook, you can even restrict content to certain friends)
- You shouldn't befriend, give details to or agree to meet up with anyone you meet online who you don't know – it's easy for someone to make an account with fake details. If in doubt, ask a trusted adult
- Use messaging, microphones and/or webcams responsibly and only to communicate with people you know and trust. This includes not participating in "sexting", or behaving in a way that is rude or abusive to others
- Avoid using your real name where possible (such as on forums or message boards), and be careful about what personal information you post online – if others can see it, they could gradually piece together enough information to gain access to your accounts. You should also not publicly post when you are going away, as this can make your house a target for opportunists. *Note: Your privacy settings should also be set high enough that only your friends can see what you post*
- If anything or anyone online makes you feel uncomfortable or worried, you should stop what you are doing (and turn off the computer if you want to) and tell a trusted adult immediately.

Browsing the web:

- Be careful to only visit websites that are trustworthy and that you are familiar with; if in doubt, ask a trusted adult
- Don't open email attachments from people you don't know, don't provide people or websites you don't trust with your email address or personal data, and don't click on anything (e.g. links, downloads, adverts) unless you're sure it's safe; if in doubt, ask a trusted adult
- You shouldn't give your details to, or communicate with, anyone that you don't know without permission from a trusted adult
- If anything or anyone online makes you feel uncomfortable or worried, you should stop what you are doing (and turn off the computer if you want to) and tell a trusted adult immediately.

Cyber Security

Passwords: It's extremely important to ensure that any passwords you create for your accounts are secure and not easy to guess. Here are some tips for creating a secure password:

- Use a combination of symbols (e.g. £, #, *, or even a space), capital letters, lowercase letters and numbers
- Don't use the name of something or someone important to you, as this may be easier for others to guess
- Don't share your password with anyone – not only could they access your account, but they could (even unintentionally) pass it on to someone else. If someone else accesses your account, they could access your personal data, and even change your password so you can't access your account (without other methods, such as security questions or password reset)
- Don't write your password down anywhere where others could find it
- Be careful about what personal information you post online – if others can see it, they could gradually piece together enough information to gain access to your accounts. *Note: Your privacy settings should also be set high enough that only your friends can see what you post.*

Viruses and malware: It's important to ensure that malicious software doesn't affect your computer or compromise your personal data. Here are some tips to prevent viruses and malware:

- Use trusted anti-virus software, keep it updated (as updating its database can protect against new viruses and malware) and run regular scans (once a week can be good; you could schedule these scans to take place automatically. It's also a good idea to perform scans when you're not using your computer, as they can slow it down)
- Keep your operating system up to date, as updates can include important security updates
- Make sure your network is password-protected and uses WPA or WPA2 encryption
- Avoid using open Wi-Fi networks
- Don't open email attachments from people you don't know, don't provide people or websites you don't trust with your email address or personal data, and don't click on anything (e.g. links, downloads, adverts) unless you're sure it's safe; if in doubt, ask a trusted adult.

Another important tip: Lock your computer when you're not using it. On a Windows 10/8/7 PC, you can do this quickly and easily by pressing **Windows Key + L** at the same time. Other types of computers can also be locked; this option is usually found in the equivalent of the "Start" menu.

Useful Resources

These resources can provide useful information about online safety and cyber security for a range of audiences. You can read what each resource is about below, and click on the hyperlinked (bold and underlined) text to visit the resource.

CEOP is the "Child Exploitation and Online Protection command". This page provides information on how to make a report to CEOP; you can make a report yourself, or, if you're worried about someone else, you can make a report for them.

Thinkuknow is a website provided by CEOP that provides information, games and resources for different age groups, as well as parents, carers and children's workforce. There is also a "Report Abuse" button which links to the above CEOP page.

This NSPCC site (in partnership with O2) provides information on keeping children safe online. There is also a section with resources for schools and teachers which you can find by clicking **here**.

Net Aware is run in partnership by the NSPCC and O2 and provides useful information about apps, games and social networks to help keep children safe online.

Be Internet Awesome is a program run by Google that aims to teach children about digital citizenship and having confidence online. The website includes resources for educators and families, as well as an adventure game called **Interland**, which includes themes of digital safety and citizenship.

The **Glow Community Rules** support learners, teachers and parents in developing an awareness of online safety and to help them in positively using Glow and the Internet.

You can also view the **UK Government's National Cyber Security Strategy 2016-2021** (also **here**) and the **Scottish Government's National Action Plan on Internet Safety for Children and Young People** (also **here**).

Cyber Skills Lesson is a website with several activities which can provide an interesting insight into cyberattacks and security.

RespectMe, Scotland's Anti-Bullying Service, also has specific information about online bullying; you can find a page with information about online bullying for adults by clicking **here**.

Stay Safe Online from Police Scotland contains online safety tips for 9-12 and 13-16 year olds.

Education Scotland's Internet safety page has online safety information for staff, pupils and parents.

360˚ Safe is an e-safety self-assessment tool designed for Scottish schools, which is also available in the Glow App Library.

The **UK Safer Internet Centre** is a partnership of online safety organisations which offers advice and resources, as well as a "Professionals Online Safety Helpline" (0344 381 4772) to help anyone working with or for children with online safety issues for them or any children or young people in their care.

This **Education Management Circular** from Argyll and Bute Council contains advice on online safety and cyber security, as well as guidelines specific to Glow and Internet use in schools.