Online safety

Staying safe online is not something that occurs automatically. Everyone needs to take responsibility for what they do and don't do. *Digital resilience* is the term for understanding the relationship between technology and risk, and being positive about dealing with it.

Teachers and learners can contribute to staying safe online by (in alphabetical order):

- backing up documents and data to a separate drive or to the cloud
- being aware of scams (a dishonest scheme or fraud)
- being careful when using Wi-Fi networks as others might be able to access their device and its contents
- changing passwords regularly; making them complex and not revealing them to anyone
- checking the origin and authenticity of posts which might be fake news or untrue
- checking the privacy settings of social networking sites so as not to reveal anything personal to strangers
- covering a webcam when it's not in use
- following relevant policies, procedures, codes of practice and legislation
- keeping personal and professional networking accounts separate
- not accessing insecure or untrusted websites
- not clicking on links or attachments unless they are from a trusted source
- not getting too friendly with someone online, or meeting strangers in real life, as they might not be who they say they are
- not posting anything in a public forum which you would not willingly say to a total stranger
- not purchasing anything from an insecure site
- not uploading pictures or videos of yourself unless you are happy that other people can access and use them for purposes you might not have intended
- only using the communication channels provided by your organisation i.e. a secure email account, or password protected VLE or intranet
- reporting sites or users which you are seriously concerned about
- thinking before you post something; once your text and/or images are online, they might be accessible for many years, even though you think you have deleted them
- using anti-virus and/or anti-spyware software and a firewall to stop unauthorised access to a computer or a device and its contents.

An aspect to consider when using computers, devices, keyboards and accessories which are shared amongst others, is hygiene. Germs can linger and then be caught and spread by everyone who uses them. Washing hands regularly, and/or using cleansing wipes or antibacterial/antivirus liquid can help to prevent this. Having good hygiene is something to be aware of, particularly in times of a virus outbreak, and/or coughs and colds.