Staying Safe online

We spend a lot of time on computers and other smart devices, whether it's doing research for their assignment, looking up resources or sending emails to lecturers, colleagues and students. There are many ways that you can ensure your data is kept private, your identity protected, and you remain safe online.

Use official email addresses or social media accounts

Whenever you are interacting with your College, make sure to check that you are using official College email addresses or contact information. Do not respond directly to any emails that look like they have been sent by a College staff if the email address does not look correct.

When it comes to social media, make sure you follow official channels run by the College such as OSC Connect or Microsoft Teams.

Check your protection software regularly

When using a personal computer, ensure an enterprise-grade security software (Norton 360, McAfee etc) is installed on your device. You should scan your device regularly for malware and bugs regularly to keep your devices safe. These programmes can check for any dangerous viruses working in the background of your devices that you might not notice otherwise. They also have a range of firewalls and VPN safety offers that can keep you safe when you are on the internet, too.

Do not log into unsecured networks without protective software

An unsecured network is another name for free, unregulated wi-fi. You'll usually be using an unsecured network if you log into the free wi-fi of a restaurant, shopping centre or any other public space. Although it can be convenient to use free wi-fi, remember that it is not regulated by anyone and therefore can be unsafe.

If you do need to use an unsecured network, make sure that you have security software enabled on your smart devices. The wi-fi on the College campus is secure because you will need to use your student ID to log in, but make sure you are still running protective software to avoid any unauthorised downloads or the like.

Back up your work safely

Every time you back up your work, it creates a new copy of everything on your device. This unfortunately includes any viruses or malware that you may have unknowingly downloaded. Make sure you always run a virus scan before you back up your work to ensure that you have saved a safe version of your device.

Don’t fall into the trap of backing up too often. Find a regular schedule that fits the amount of work you are doing, and this will avoid having too many copies of your work that could be stolen or hacked. Once you find a backup system and schedule that suits you, you can ensure that your assignments and course notes are kept secure and private.

Use strong and unique passwords

It’s common for people to use the same passwords for multiple accounts, but this makes it easier to break into your accounts if a hacker has discovered one of your passwords. So, use strong passwords that are unique to each account to reduce the chances of being hacked. If you ever get a notification saying someone is trying to log in to your account and it’s not you, do not allow them access and change your password as soon as possible to ensure that your information is kept secure.

Do not click on suspicious links or download files from unknown sources

If you have protective software, it will let you know when a download is suspicious or dangerous. However, it is best practice to avoid downloading or clicking on anything that looks suspicious or has come from a source you don’t recognise.

Always check the address that the email is from and don’t click on any internal links or downloads from a sender you do not recognise.

Be aware of data-stealing and phishing

Just like links and downloads, phishing emails or phone calls can also put your data at risk. Whether it asks you to respond, share details or call a number, be aware that if it is an unrecognised source (sometimes asking you to respond with a time limit), it is likely a scam trying to steal your data.

You can always confirm a source by contacting them yourself. Whether it is the College or your bank, they will have an official number that you can call and confirm if the email is from them. Never answer immediately and start sharing your information.

Don’t download apps or extensions from unknown sources

Most students will have a range of apps on their phone, whether they are study apps, budgeting apps or social media apps. However, be wary of websites that offer you apps or downloads from an unrecognised source. Apple’s app store and Google Play store should have the app listed if it is officially registered, and you can see reviews, check comments from other users and make sure it is downloaded from a safe location.

Close accounts that you don't use any more

Everyone has multiple accounts, perhaps old emails or logins for websites that we no longer use. However, it's important to close these when you no longer need them. Leaving an account open is another location for your data or contact information to be taken from.

This can apply to everything from online resourcing tools, shopping accounts, memberships and student software. If you don't use it and won't again in the future, consider closing the account down.

Turn off networks when you are not using them

There are forms of hacking and viruses that can infect devices even when you are not actively using them. To keep this from happening, it's best to switch off any networks when you are not using them. It will also give your antivirus software a chance to scan everything and start fresh the next time you begin to surf the web.

Use of social media apps

Data is not just something that can be stolen through hacking or viruses. Nowadays, everyone lives on social media, and we like to share what we are up to with our friends and family. However, if you have public accounts or have contacts you don't know that well on your accounts, oversharing can be dangerous.

Parents must be vigilant and proactive in overseeing their children's use of social media applications such as TikTok, Bigo, Instagram, Snapchat, WhatsApp, and other platforms. It's crucial to comprehend the apps' full capabilities, adjust privacy settings appropriately, and guide children in responsible online conduct to shield them from unsuitable content.

The rise in the use of abbreviations during conversations when using social media applications, especially among children, poses serious risks. It's important for children, parents, and educators to be aware of the potential dangers. Some of the examples of common abbreviations in use are:

Abbreviation	Meaning
Beta - Bux	A Man who uses money to keep a woman
FYEO	For your eyes only
55555	Crying my eyes out
DOC	Drug of choice
LMIRL	Let's meet in real life
NIFOC	Naked in front of camera

Parents should guide their children to communicate clearly and steer clear of abbreviations such as 'lol', which might lead to misunderstandings.

Additionally, safeguarding issues such as drug taking, alcohol misuse, and sharing of inappropriate images can put children at risk. Awareness of these issues is crucial for all to protect children from harm.