Working from home and staying safe online

During these unprecedented times, we understand that teaching and support staff have had to make adaptations to how they teach and work, as working online becomes the 'new normal'.

Here are a few important things to remember when working online:

1. Accessing college systems at home

Please remember you can access your College desktop, all your usual documents, and College systems, via the secure Remote Desktop site (guidance here).

- You can also access iTrent, Skype for Business, and Moodle directly and securely (guidance here).
- Please avoid saving College documents directly on to your personal laptop or home computer's own drives unless absolutely necessary.
- Be aware of your environment - use headsets for phone calls or online meetings where available and lock your computer when not in use.
- For guidance on the use of Microsoft Teams please use the Microsoft Teams Resources & Guidance on Moodle Staffzone.

2. Use of Zoom

Where you are using Zoom, please:

- Ensure your Zoom app is updated - https://zoom.us/download - as the newest version offers encryption.
- Ensure you sign up using your Edinburgh College email address.
- Ensure that ***Meeting Passwords*** are required to join your meeting; and that they are not shared in an uncontrolled manner (e.g. via social media).
- Use the ***Waiting Room*** feature to have participants wait until the host arrives and vet participants prior to entering the meeting.
- ***Lock*** your meeting once it's started, so that no one else can join.
- Don't use social media to share conference links as malicious groups can search social media for these meeting ID/links.
- Allow only signed-in/registered users to join: If someone tries to join your meeting and isn't logged into a Zoom account, they will receive the message 'This meeting is for authorised attendees only'.

- Turn off file transfer: In-meeting file transfer allows people to share files through the in-meeting chat. Toggle this off to keep the chat from getting bombarded with unsolicited pictures, GIFs, memes and other content.

Further security information and tips for secure use of Zoom is available on Moodle Staffzone.

3. Emails, BCC & Data Breaches

The sending of emails to the wrong recipient was the second largest cause of accidental data breaches reported by the Information Commissioner's Office (ICO) in their latest figures. When working from home:

- Please remember to double-check you are sending emails to the correct recipient(s) – review the "TO", "CC" AND "BCC" fields before clicking send.

- Always use "BCC" if you're using students'/individuals' private email addresses; or if you need to keep the names or email addresses of recipients private (for example, because the email is about a sensitive matter and disclosing the distribution list would cause emotional distress or embarrassment).

4. Phishing scams

Cyber security experts and Police Scotland have found that COVID-19 has led to a surge in phishing scams, with both individuals and organisations at risk, so it is important that we all remain vigilant and are aware of cyber threats.

- Staff should double check requests - for example call colleagues to confirm a request that has a financial implication (or may cause a data breach if released to the wrong individual) even if the email looks genuine.

- Trust your instinct – if something does not seem right, it probably isn't. Think before you click!

5. Use of social media (Facebook, Twitter, Instagram, WhatsApp – any other social and messaging platforms)

When communicating via social media channels as a member of Edinburgh College staff it is important to apply the same standards online as you would when face-to-face. Be considerate when posting content or exchanging individual or group messages.

- If you are posting content or sending messages which invite responses, stay engaged with the content to ensure that all dialogue, images, video content and links which may appear are respectful and appropriate to **ALL** those involved.
- Check the accuracy and sensitivity of the content that you are communicating before pressing send or posting.
- Make sure you have permission before using someone else's images or written content publicly.
- Please remember that once something is posted online, it can be difficult to remove or retrieve. If in doubt, don't post.

- When posting, speaking, or sending a message in a personal capacity using a personal account which associates you with Edinburgh College, use a disclaimer such as: 'the views expressed here are my own and in no way reflect the views of Edinburgh College.'
- When communicating individually with students on social media platforms, please ensure that the students are aware of professional boundaries and the appropriateness of communicating during usual College hours.

More information:

If you any queries relating to data protection, please email: dataprotection@edinburghcollege.ac.uk

For any support, advice or questions in relation to software and use for learning and teaching please contact the Learning Technology team via the Moodle helpdesk: moodle@edinburghcollege.ac.uk

If you have any queries relating to online security, please email: itrequest@edinburghcollege.ac.uk

If you any queries relating to the use of social media, please email: communications@edinburghcollege.ac.uk