Data Protection & Working from Home

DCU Data Protection Unit

18 March 2020

Top Tips

- Only use the encrypted device provided by ISS, where one has been issued to you.
- If you are using a device provided to you by DCU, do not allow any other person to use the device.
- If you are using a shared device, ensure that you log out of all DCU email accounts, programmes, systems, etc., before any other person uses the device.
- Be sure to use VPN (Pulse Secure) at all times.
- Ensure that you lock your screen any time you step away from your laptop/computer. (On Windows laptop and computer keyboards: hold down the **Windows key** + **L** at the same time.)

- Ensure that you only save and store folders and files to your DCU Apps Google Drive (cloud storage) or to the DCU network (e.g. on the 'Business Applications' *V: Drive*) - Never save or store items directly to your device.
- Ensure all electronic documents and files are password protected.
- When engaging in calls (by phone, Zoom, Google Hangouts, etc.) use discretion and, if possible, take these calls in a separate room, away from others in your household.

Devices

- Take extra care that devices, such as phones, laptops, or tablets, are not lost or misplaced.
- Do not use USBs or other similar storage devices, as these can be easily lost.
- Ensure any device you are using for work has the latest necessary updates installed, such as operating system updates (e.g. iOS or android) and software/antivirus updates.
- Ensure your computer, laptop, or other device, is used in a safe location. For example, ensure it is kept where you can keep sight of it; and minimise who else can view the screen, especially if working with sensitive personal data.
- Lock your device if you do have to leave it unattended for any reason.
- Make sure your devices are turned off, locked, and stored carefully when not in use.
- Use effective access controls (such as multi-factor authentication and strong passwords) and, where available, encryption to restrict access to the device, and to reduce the risk if a device is stolen or misplaced.
- When a device is lost or stolen, you should immediately inform the DCU Data Protection Unit and ISS, and take steps immediately to ensure a remote memory wipe, where this is possible.
- If it is unavoidable and you must use your own personal mobile phone or other personal devices, please ensure that you password protect your devices, and that you change your password(s) regularly.
- Equally, if it is unavoidable and you must use your own personal devices to store data, please ensure that you password protect and encrypt this data.

Cloud and Network Access

- While working from home, please only save and store documents on DCU's cloud storage and/or on DCU's secure network, as appropriate.
- Only use DCU's secure network and DCU's Google Apps for Education cloud services.
- Comply with organisational rules and procedures in relation to cloud or network access, login and, data sharing, including restricting access only to those staff who require it

Physical data security

- If it is the case that you have brought physical files with you to home, and/or you must print documents while working from home, please ensure that these are kept secure at all times.
- While you are working, please ensure that any physical files are kept within your sight.
- When you are finished working, please ensure that physical files are locked away in a secure location in your home – such as a lockable cabinet, bedside locker, briefcase, or in a lockable room.

Emails

- Follow existing DCU policies around the use of email.
- Use your DCU staff email account for work-related emails. Do not use any personal email accounts for work-related emails.
- Avoid using personal or confidential data in email subject lines.
- When emailing multiple recipients, ensure that the recipient email addresses are in the BCC field, unless you have a legitimate reason for sharing the recipients' details with one another.
- Before sending an email, check and double-check to ensure you're sending it to the correct recipient(s), particularly for emails involving large amounts of personal data or sensitive personal data.

Further guidance

See also: **DCU ISS web page on remote working**