General Data Protection Regulation
Staff Guidelines

Background

All staff must comply with the requirements of the college's Data Protection Policy. As part of the General Data Protection Regulation (GDPR) the College needs to review some of its practices to ensure compliance.

Whilst much of the GDPR work surrounds how electronic data is stored or how data collected in other mediums is secured, staff also need to consider information security in other aspects of their work and on-line presence.

This list below is not meant to be exhaustive but is aimed at increasing awareness of information security: how something that seems innocuous can lead to a breach of data security.

Please read the list and take a little time to think how this affects your working life & practices. Rather than think of the data as being personal to a student or staff member, imagine it is some information that is personal to you and project that image into the scenarios.

Remember – security of our data lies with all staff under the GDPR guidelines. Staff must take all reasonable steps to ensure the security of any personal data relating to college employees or students, (either future, current or past) to which they have access. Information should not be disclosed to any person or organization unless there is a legal, contractual or vital public interest in doing so.

In College

- Lock your computer when you leave it unattended,
- Shut your computer down at the end of each day,
- Move any sensitive information off your desk and lock it away if you are leaving your work area,
- If you have removable media in your computer remove them and lock those away as well,
- Before you throw a piece of paper in the bin, stop and consider what is on it. Is there sensitive data? Does it include information, say name and address or contact details of someone? If yes then either shred it or put it in the confidential waste bin.
- Don't leave laptops, tablets or other removable media unattended,
- If you **need** to take sensitive information home, use an encrypted USB stick. The new Foldr should almost entirely remove the need for USB sticks.

- When printing off information that is of a sensitive nature retrieve it from the printer immediately.

- Try to avoid using a password on work information that is the same or similar to your personal information – ie don't use your bank password for documents at work,

- If you receive an e-mail that you're unsure of, either through a link on an e-mail, or via tweets and posts take care. If you're suspicious or have any doubts delete the e-mail and inform CCIT.

- Be aware that cyber criminals are changing their method of communication so that they e-mail a scenario to you asking for help or stating something is urgent – before you act, think and question whether it looks legitimate and ask for advice before passing over any information,

- Don't automatically send information to external stakeholders, even when they are people you have dealt with before. Confirm with them the security of their systems, how they intend to use the data and ask for their GDPR policies / data security accreditations,

- Don't save passwords on machines where there could be multiple users (hot desk at work) or on laptops or your home computer where others may have access to the machine and could sign in as you. If something comes from your e-mail or mobile device it is assumed to be from you.

<u>Mobile Devices</u>

- Use strong passwords and touch ID features and lock your devices when not in use.

- Before downloading an App think of the data it may have access to. Information on you, your contacts, location and where you shop all has value so be mindful before giving up that information,

- Public Wi-Fi spots tend not to be secure so take care what you do when you connect to them. Avoid logging into sensitive data areas, be that work–based or personal, as others could potentially see what you are doing,

- Keep your computer, phone and apps up to date. The college computers will be updated through the IT systems but ensure your personal devices are up to date to avoid the risk of viruses / malware getting through,

- Once you're finished with an App – delete it. You can always download it again for free later.

<u>Working Off-site or at home</u>

- If you need to take work offsite, consider what you need and why you need it,

- Only take the minimum amount of information,

- Ensure the device / paperwork is out of sight – lock it in the boot – it takes no time for someone to smash a window and remove items from a car – even one at a petrol station. Take the information out of your car as soon as you get home.

- If you need to take information home on a USB stick, and the USB will have personal information on, only use an encrypted USB stick. Foldr should almost entirely remove the need for USBs.

- Take care with paperwork you discard at home as you would at work – does it need to be shredded?

- When you come back into work bring back as much of the information you took home as possible. Ask yourself the question – will I need that again at home or should I take it into work and dispose of it securely?

Emails

- Most data breaches occur with emails.

- Make sure you send to the right person

- Encrypt if it contains personal data sent externally

- Don't CC other users in-use BCC.

Related Policies

These can be found on myLoreto

- Data Protection Policy-GDPR-May 2018

- GDPR Policy Exams-May 2018

- CCTV Policy-May 2018