STEP FOUR

Ensure secure access to our office environment

Is your Office Secure?

Below are some of the key areas that can be at risk in your office environment, here are some ways you can reduce this risk:

Unlocked PC/ Laptop
When you leave your desk, make sure you lock or log off your PC/laptop otherwise this will allow direct access to our network

Passwords
Ensure that your passwords aren't written down and left in your office (i.e. stuck on your monitor, under your keyboard etc.)

Clear Desk
When you leave your desk, make sure confidential papers aren't left on your desk

Unattended Mobile Devices
If you leave your desk, secure or take your mobile devices such as mobile, USB stick, iPad etc. with you

Lanyards
Keep your lanyard with you at all times and be prepared to challenge strangers in your work area!

Disposal of Confidential Information
Dispose of confidential paper appropriately shredder/ confidential waste bins.
The College is required by law to hold key college documents including personal data for set periods of time. Electronic files held in personal areas of the network should be deleted in the standard way by the department generating the date and in line with the retention policy.

STEP FIVE

Protect our information from fraud

Phishing

Emails from hackers will look legitimate at first glance so it is important that you treat any email you didn't expect with suspicion. Make sure the email is genuine before you click on any links or open any attachments! Don't trust the display name of the email, check the email address in the "from" address and hover over links before clicking them to see if the web address is legitimate and relates to the email's content. Check for odd phrases and word choice based on your knowledge of the sender, is there a lack of personal greeting or phrases aimed at manipulating you? For example, an email could be made to look like it is from your Manager. Always speak to them if you have doubts about its content.

Targeted Spear Phishing

Hackers identify individuals via social media sites and use these to gather data about you. They utilise your hobbies, partners, children, pets and holidays. Hackers then send specific, personally crafted emails to individuals designed to target their vulnerabilities.

Phone Phishing

Callers impersonate a customer to phish for details and apparently innocuous information. The criminal may use the information gathered to trick a real customer.

Ransomware will send you scam emails (or disclose a website to encourage you to download a file) with links or attachments that will install a type of malware on your PC. This malware will prevent or limit you from accessing your system, either by locking the screen or by locking your files unless a ransom is paid.
For more information on spotting phishing emails and other security tips, visit
https://thehub.kendal.ac.uk/itsupport

Don't click on a file that you are not expecting, or a file that is on a suspicious email or website.

5 STEPS TO KEEP YOUR INFORMATION SECURE

Kendal College
a brighter future

STEP ONE

Confidential information

Data Classification

Public - Information that has already been published.

Internal – Information that can be disclosed to all employees or affiliates.

Confidential – Sensitive information whose access is subject to restriction. For example: Customer and colleague information, bank card data, sensitive company information and passwords:

- *For confidential documents, ensure the footer includes the word "Confidential"*
- *Confidential paper documents should be stamped with the word "Confidential"*

If in doubt
don't share and consult your manager.

Managing a personal data breach

All incidences of breach must be reported to DPO who will decide on action to be taken including the requirement to notify the ICO within 72 hours of the report.

Rights of Individuals

Individuals have a range of rights in respect of their data including access, rectification, erasure, objection. All requests must be referred to the DPO and responded to within a month unless the request is complex in which case the period may be extended up to a further two months

STEP TWO

Ensure secure access to our buildings and devices

Device Security

Keep Devices Safe

When travelling with laptops, mobile phones, iPads, USB sticks etc. ensure that these devices are protected against theft. Don't leave devices in cars whenever possible. If you need to leave them in the car, ensure that they are not on view. Take your laptop and phone home with you from the office each day to reduce our information Security risk but also enable us to ensure that business continuity and disaster recovery plans can be implemented if needed. Always use a Pin or a Password to start the device.

Lost Devices
Report any lost devices to the IT Service Desk as soon as possible so that we can work with you to protect both your information and the company's information.

Ensure Secure Access to our Buildings

Badge Surfing

All staff, students, guests and contractors should wear lanyards at all times. Politely ask unknown colleagues & guests to return to reception and sign in.

Call the Estates team to report any suspicious activity or actual security incidents so that we can better protect the work environment.

If you don't know someone
challenge them, or contact the Estates or management teams

STEP THREE

Ensure secure access to our information

Passwords

Hackers use passwords to get access to personal and company information. The most commonly used types of password include "123456", "password123", pet names, family member's names and dates of birth. These are all weak passwords. A strong password is the first defence against cyber criminals.

Creating Strong Passwords

- *Length is key! Make it long and use random words, using a combination of letters and numbers e.g. Give6pencils2U!*
- *Don't reuse passwords, use unique passwords for important accounts*
- *Never share your password with anyone*

If you think your password has been hacked, change it for all accounts where you use that password. Avoid using the same password for multiple online accounts.

Public WIFI

When accessing Public WIFI, be mindful that the connection is not secure. Only work on confidential tasks when you're at home connected to the company network or in the office.

Access to Information

Ensure that only colleagues who really need access to certain information to perform their role are able to access the relevant folders and applications. Even meeting rooms are "unsecure". Make sure any meetings with confidential content are conducted in a way that only authorised colleagues have access to the information.