IEC's Data Risk Avoidance Procedures

Introduction:

The purpose of this document is to detail the procedures implemented by IEC to minimise or avoid, in as much as is possible, the tasks that could result in a data breach. A core idea that informs the College's data protection policy and procedures is the goal to avoid potential data protection issues in as much as is possible.

Rationale:

The impact of a data breach that is deemed high risk would be very serious for the data subjects affected. As a data controller, IEC has a responsibility to ensure that the data that it acquires of its data subjects is used and maintained in a secure environment. These procedures are intended to help IEC prevent such data breaches through an active avoidance policy.

Scope:

This reference document provides a set of procedures that IEC staff will implement, with the goal of instigating work processes that have risk avoidance of a data breach as a core consideration.

This policy should be read in conjunction with the associated Data Protection Policy, Subject Access Request procedure, the Data Retention and Destruction Policy and the Data Retention Periods List.

Data Risk Avoidance Procedures:

The following have been highlighted as the main potential sources of data security breaches:

Internal threats:

- Unsecured data – e.g. data that is left on someone's desk
- Saving data to personal accounts/drives
- Emails
- Loss of hardware – e.g. an unsecured laptop
- CCTV – Need to ensure signage alerts people to this, and need to take care of how/where it is stored. In the case of hard drives storing CCTV offices need to be policed at all times or offices of the building locked.

External threats:

- Hacking
- Malware/ransomware

The data risk avoidance procedures outlined below have been informed by consultation with various sources with the goal of minimising the potential impact of these key risks, and to put in place a procedure that avoids this risk.

Procedure	Rationale
Avoid sending email attachments for internal emails	A common risk for businesses is sending attached files that contain personal information of data subjects. By sending links to a file on an internal share drive rather than an email attachment, such a risk is minimised
Remove auto-fill of email addresses when writing an email	A common reason as to why an email is sent to the wrong person is that the email application has auto-filled the recipient based on prior emails, even though the auto-filled email address is not the intended recipient
Ensure computer operating systems and all software are kept up to date and run antivirus software regularly	A common external risk is malware or ransomware. Keeping operating systems and software up-to-date, and running antivirus software regularly, ensures that this threat is minimised
Ensure all electronic devices that are used for work-related to College activity are password-protected	The loss of hardware, such as laptops or mobile phones, is another common data breach occurrence. If such hardware is password-protected, then the loss of hardware does not necessarily mean that there will be a data breach
Lock computers when they are unaccompanied	If a computer is left 'open' when it is unattended (e.g. during lunch break), then the potential for personal data to be accessed without permission is evident
Minimise printing of documents or emails with personal information	If such documents or emails are printed, then the risk of the loss of a hard copy is present. As a rule, the creation of hard copy records of personal information should be avoided
Shred hard copy records when they are no longer needed	If a hard copy record of a document or email that contains personal information is created, it should be destroyed by shredding, once the purpose of its creation has elapsed. This procedure should be cognisant of the IEC Retention Periods reference document
Minimise the use of personal data for work processes	If a work process requires the use of personal data, ensure that the least amount of personal data is provided to fulfil the purpose of the process – i.e. do not give more personal data if it is not required of the purpose of a process
Clear desks	The creation of hard copy records allows for the potential of a data breach. The likelihood of such a breach is heightened if such records are not securely stored for the duration of their purpose. A common example of such is if hard copy records are kept on an employee's desk. A clear desk policy reduces this risk
Saving of work material	If work related material is not saved to a secure location, the risk of a data breach is heightened. Common examples of unsecure locations would be to an individual computer's desktop, or to a personal cloud based server. Therefore, to reduce this threat, all work related material should be saved to the appropriate College share drive, as these are secured and have limited access