KIRKLEES COLLEGE

Working at Home Data Security Guidelines

This guidance is intended for all staff that work at home, either on an occasional or a regular basis. It applies to anyone undertaking administrative or teaching-related work at home.

This guidance gives general advice on the issues you need to consider ensuring that any College information you work on at home is protected from loss or unauthorised access and exploitation, while also ensuring that it is accessible to anyone that needs to use it if for their work. It applies to information in all formats, including paper files, electronic data, word processed documents and e-mails.

The Data Protection Act 2018, General Data Protection Regulation and the Freedom of Information Act 2000 apply to all information that you receive and create as part of your employment with the College, regardless of where you work or store that information.

The Data Protection Act permits people to see information that the College holds about them while the Freedom of information Act gave people the right (from 1st January 2005) to access any other recorded information that the College holds. The Data Protection Act also requires us to hold information about living identifiable individuals for no longer than is necessary, to ensure that information is accurate, and to ensure appropriate security measures for this information to protect it from unauthorised access, amendment or deletion.

The primary copy of College information should ***not*** be stored at home, so College records should be updated as soon as possible with copies of any work that you do at home. This applies to all teaching or administrative work. This allows anyone who needs to refer to the records in your absence to be able to access the most up-to-date information. It will also ensure there is a backup copy of the work, if you were to lose your work at home. Finally, it will enable the College to respond to any Freedom of Information or Data Protection request for that information without having to ask you to search information you have at home.

You will need to take reasonable measures to protect the information from unauthorised loss, access or amendment whilst stored at home. This will enable the College to comply with our Data Protection Act obligations and is also in the College's business interests: depending on the nature of the information involved, if someone inappropriately gained unauthorised access to College information it could cause reputational, commercial or competitive damage to the College. For example, sensitive information about students or staff, or the exploitation of another person's work.

Electronic data should preferably be accessed from a college owned device, although in some instances personal devices can be used following prior approval by your HoF. Depending on the application, connection to the college systems and resources should be via either a Virtual Private Network (VPN) installed by IT on your college issued device or via a secure web connection (https:) VPM ensures a secure connection between your home broadband connection and the college network. Both methods will ensure that when you work at home you will not need to take any measures with regard to electronic information and your principal concern will be to protect your paper information.

The paper information you use at home is most vulnerable to loss or unauthorised access in the following ways:

- As a result of leaving papers in household areas where they may be seen by other members of your household or by visitors. This is most likely to cause difficulties when the information is about identifiable individuals.
- As a result of crime e.g. theft
- As a result of loss, particularly on the journey to and from work

All paper information must be held securely within the home environment.

Copying personal data to a memory stick or emailing data to non-college email addresses is strictly prohibited as this makes the data more vulnerable to loss or unauthorised access or amendment in two ways:

- Physically, through the loss, damage or access to the storage medium on which the information is held, most commonly loss of flash drives.
- Remotely, through someone accessing (hacking) your computer while it is connected to the Internet or through a virus.

When deciding what reasonable security precautions you need to take against these vulnerabilities, it is necessary to balance their financial cost, time and practical implications against the seriousness of the damage that would result if someone did see the information or made unauthorised alterations to it. Depending on the nature of the information, this damage could entail **legal action against you or the College, damage to the College's or your reputation; or damage to collaborative relationships caused by the inappropriate release of information.**

You should **never use non-College e-mail and cloud storage accounts for College business**. College e-mail accounts and the College Office 365 applications such as OneDrive and Teams are accessible via any Internet connected browser.

If you require any further information or support please contact Jonathan Wilkinson JWilkinson01@kirkleescollege.ac.uk or IT support on 01484 43(7016).