Information Security Good Practice Policy

Introduction:

We would like to remind you of the importance of maintaining Information Security vigilance in your day to day activities, both at work and away from the College.

Please read through the list below to help ensure both the College and your personal information remain secure.

We want you to follow the instruction below:

- **Read the Information Security Policies**

Do	Know what your responsibilities are and what to do should the worst happen.

- **Protect your user accounts**

Do	Use strong passwords and keep them secret. Passwords should be a minimum of 12 characters including Capital, lower case, numbers and a symbol
Do	Report compromised user accounts to Select Technology promptly
Don't	Use the same password on multiple IT systems
Don't	Use your College email or login details to register on 3rd party hosted IT systems/sites or those used for personal purposes e.g. shopping stores, social media and cloud services.
Don't	Use your College password for a 3rd party IT system approved for use by the College authentication unless it authenticates you via the College's Portal.

- **Protect your computer**

Don't	Install illegal software on your work computer
Don't	Connect unknown personal devices to your work computer
Don't	Connect your personal device to the College's network or to a work computer
Do	Shut down your work computer at the end of work
Do	Lock your computer screen when absent from your desk

- **Use and handle information with care**

Do	Store work related documents on the relevant SharePoint site and not the local drive (C). Your OneDrive should be used to store work documents that do not require access by other colleagues. Store confidential papers in lockable drawers when absent from your desk.
Do	Do not use USB sticks or other storage devices on college devices.
Do	Where feasible, password-protect confidential documents before emailing them.
Do	Mark sensitive emails and post with Private and Confidential and seal postal mail securely.
Do	Check that your documents have not been left on desks, printers or in meeting rooms.

Do	Ensure that your desk is clear of all paper before leaving for the day. If you are using a hot desk please ensure you take all papers with you.
Don't	Access unapproved file storage/sharing apps or services to store/share College data.

Reordered the above for clarity - so the 'Dos' and all together

- **Use email with care**

Do	Verify the email source before you open its attachment or the link included.
Do	Confirm a recipient's email address before clicking Send.
Do	Remove confidential information in email messages particularly when forwarding emails.
Do	Delete confidential emails received in error immediately and notify the sender.
Don't	Enable auto-forwarding from your work email to your personal email.

- **Use the internet with care**

Don't	Connect to unfamiliar Wi-Fi networks
Don't	Use confidential information on social networks
Don't	Visit sites that may violate College policies or are flagged to be untrusted.
Don't	Access any website, share or download files that may violate the College's policies

- **Others**

Do	Take extra care to protect College information and mobile devices when working off site.
Do	Read the College's Information Security and Information Compliance Policies and procedures.
Do	Report any suspected or actual information security incident immediately to Select Technology

Select Technology details:

support@select-technology.co.uk

Document Control:

Document title: **Information Security Good Practice Policy**

Version	Author		Reviewed/Authorised	
	By	Date	By	Date
1.1	Kerensa Gardner & Maggi Knights	July 2020	Luis De Abreu	25.09.2020
1.2	Kerensa Gardner & Russell Gower-Leech	December 2023		

Issue: **1.2** Date of current issue **05.12.2023** Date of next review: **31.07.2024**