Information Security Policy

The following policy has been drafted for the approval of the CECOS Board of Governors. Any amendments to the policy require the Board's approval. Each Centre or campus and department within CECOS College is required to comply with this policy. Support and guidance for Centre's and departments is offered by the College's Director of Communications and the IT and administration officer.

Information Security is not a new requirement, and to a large extent the policy and accompanying procedures formalise and regularise existing good practice within the College. This policy provides guidance on the College's information security requirements; identifies potential risks and highlights good practice. It is fully supported by the CECOS College Data Protection policy.

CECOS College is required to review this policy yearly to ensure any new developments are covered and protected.

1. Introduction

CECOS College seeks to maintain the confidentiality, integrity and availability of information about its staff, students, fellows, members, visitors, alumni, and its affairs generally. It is extremely important to the College to preserve its reputation and its integral parts. Compliance with legal and regulatory requirements with respect to this Information is fundamental. Information use will be managed in lie with the guidance provided in the Data (Use and Access) Act 2025 and only used for lawful purposes.

2. Objective

The objective of this Information Security Policy is, as far as reasonably practicable, to protect all sensitive information assets from all threats, whether internal or external, deliberate or accidental.

The key objectives of the Information Security Policy is to:

- Provide management with direction and support in relation to information security in accordance with business requirements and relevant laws and regulations.
- Promote sound information governance and facilitate effective resource management thus contributing positively to the College's vision and values.
- Protect the College's information assets from all relevant threats.
- Ensure our information security meets our obligations under the General Data Protection Regulation (GDPR), Data Protection Act 2018 (DPA) and Privacy and Electronic Communications Regulations 2003 and all associated codes of conduct in data protection law applicable to the College.

In support of these objectives all users of data assets, whether they are physical or electronic, accept their roles and responsibilities in ensuring information is protected and are committed to:

- Treating information security seriously;
- Creating a security-positive work environment;
- Implementing controls that are proportionate to risk.

Such information (for example Personnel, Payroll, Student Records) should only be stored in appropriate secure systems and locations and is subject to legal protection. All users of the

information and any ICT system are obliged, under the terms of the Data Protection Act (2018), to ensure the appropriate security measures are in place to prevent any unauthorised access to personal data, whether this is on a workstation or on paper.

This information security policy defines the framework within which information security will be managed by the College and demonstrates management direction and support for information security across the College. This policy is meant to keep information secure and highlights the risks of unauthorized access to or loss of data.

3. Scope and definitions

The scope of this Information Security Policy extends to all the information held by and related to CECOS College and its operational activities including but not limited to:

- Records relating to students, alumni, staff, members, visitors, conference guests and external contractors where applicable;
- Operational plans, accounting records, and minutes;
- Data and information generated and used in the College's research activities;
- All processing facilities used in support of the College's operational activities to store, process and transmit information;
- Any information that can identify a person, e.g. names and addresses.

This policy covers all staff where any reference to staff shall be regarded as relating to permanent, temporary and contract staff.

4. Policy

CECOS College aims, as far as reasonably practicable are to:

- Protect the confidentiality, integrity and availability of all data it holds in its systems. This includes the protection of any device that can carry data or access data, as well as protecting physical paper copy of data wherever possible;
- Meet legislative and contractual obligations;
- Protect the College's intellectual property rights;
- Produce, maintain and test business continuity plans in regards to data backup and recovery;
- Prohibit unauthorised use of the College's information and systems;
- Communicate this Information Security Policy to all staff;
- Provide information security training to all staff appropriate to the role;
- Report any breaches of information security, actual or suspected, to the Data Protection Lead (marlon@cecos.ac.uk) and the Director of Communications in a timely manner.

More detailed policy statements and guidance are provided in Section 8 of this Policy.

5. Risk Assessment and the Classification of Information

Risk assessment of information held specifically and generally relates to:

a. The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process

of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.

b. The risk assessment should identify the information assets of the College; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to the College as a whole. In assessing risk, the College should consider the value of the asset, the threats to that asset and its vulnerability.

c. Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.

d. Rules for the acceptable use of information assets should be identified, documented and implemented. Where these are held on or accessed through a computer system, the College's Regulations and Policies applying to all users.

e. Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the College's infrastructure, systems and processes.

6. Personal Data

Personal data must be handled in accordance with the Data Protection Act 2018 (DPA) and in accordance with this policy. "Personal data" means data which relate to a living individual who can be identified from those data, or together with other information which the College holds, or may hold, and includes any expression of opinion about the individual and any indication of the intentions of the College or any other person in respect of the individual. The rights of the Data Subject must at all times be respected, including requests for access to their data, transportability of data and the right to have their data erased subject to essential data management and protection conditions and conditions set out in Article 6, 9 and 10 of the DPA.

The DPA requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

A higher level of security should be provided for 'sensitive personal data', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of any offence.

7. Responsibilities

The Governing Body holds key responsibility for ensuring compliance with this policy and all data breaches within CECOS College.

The Governing Body requires the head of each department in College to be accountable for implementing an appropriate level of security control for the information processed and used by that department's members of staff. Each member of staff is accountable for operating an appropriate level of security control over the information and systems he/she uses to perform his/her duties.

The Director of Communications is responsible for coordinating the management of information security, maintaining this Information Security Policy and providing advice and guidance on its implementation.

It is noted that failure to adhere to this Policy may involve the College in serious financial loss (both by way of a fine of up to £500,000 imposed by the Information Commissioner's Office and also by

way of damages sought by an individual whose data has been inappropriately handled), embarrassment, legislative action or loss of reputation. Non-compliance by any member of staff may therefore result in disciplinary action.

8. Detailed Policies and Guidance

The following shall be complied with throughout CECOS College.

Information assets shall be 'owned' by a named section within College. A list of information assets, and their owners, shall be maintained by the Director of Communications

Access to information shall be restricted to authorised users and shall be protected by appropriate practical physical and/or logical controls.

i. **Physical controls** for information and information processing assets shall include:

- Locked storage facilities (supported by effective management of keys)
- Locks on rooms which contain computer facilities
- Securing of PCs and other devices to prevent theft and passwords to prevent unauthorised access to files
- "Clean desk" policies
- Encryption of data either transmitted or taken outside the College's properties

Logical controls for information and information processing assets shall include passwords for systems access.

ii. **Passwords and password management systems** shall follow good practice for security and use the following techniques:

- The use of strong authentication (minimum length, high complexity, non-reusable passwords)
- Users to have the ability to change their passwords at any time
- Passwords to be changed at regular intervals. A system to be in place to automate and enforce this process
- Access privileges shall be allocated to staff based on the minimum privileges required to fulfil that member of staff's duties. Access privileges shall be authorised by the appropriate information owner.
- To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.
- All access permissions will be granted, amended and revoked following a standard published access authorisation process.

Information owners shall review access permissions on an annual basis.

iii. **Access to physical information assets** – for example printed paper documents, and media containing information – shall be governed as appropriate by the same principles as above.

An appropriate leavers and joiners process shall be in place to ensure that all employees, contractors and third party users have information access permissions revoked and return all of the College's assets in their possession upon termination of their employment, contract or

agreement. Heads of departments are responsible for completing a leaver's checklist and communicating that list to appropriate departments.

The circumstances under which the College may monitor use of its ICT systems, and the levels of authorisation required for this to be done, also need to be compliant with the regulations and restrictions of partner institutions.

iv. **Access to operating system commands** and the use of system utilities - such as administrator privilege - that might be capable of overriding system and application controls, shall be restricted to those persons who are authorised to perform systems administration or management functions. Such privileges shall be authorised by the Director of Communications only in line with individual job roles and responsibilities.

v. Visitors to the College

Visitors to the College should be provided with specifically assigned credentials and should be appropriately authenticated and automatically disabled at the end of their term with the College.

vi. Use of Personal Computer Equipment and Removable Storage

CECOS College recognises that there may be occasions when staff need to use computing equipment not provided by the College to process information (including personal data). The use of such equipment for these purposes must be approved by the Director of Communications or their nominee.

The same levels of control should be put in place for information which is held on a staff members' own computing equipment or on equipment provided from outside the College or on removable storage.

It is good practice and required that:

- Computers owned by members of staff or provided from outside the College and used to process College information or connect to the College network shall have up-to-date anti-virus software installed and, if the computer is to be connected to the Internet, a firewall;
- Information shall be saved with a password or some form of encryption onto the hard drive of computers owned by members of staff where that information is personal data concerning students, alumni, or staff or other stakeholders (this would, for example, also include a reference for a student or former student);
- The information on removable storage devices shall be protected from loss and/or theft;
- CECOS College information shall not be retained on removable storage devices longer than necessary (i.e. once information that has been updated on a computer owned by a member of staff is uploaded onto College systems, it shall be deleted from the removable storage device).

vii. Email and Internet Use

The College's email systems are outsourced to the technical support services including remote support from Pakistan and CECOS's sister institution CECOS University of IT. Access to the mail server is restricted to members of the College specified by mail list owners. Staff email is the property of the College.

The College's policy and procedure on staff use of email and the Internet is included in the Staff Handbook.

viii. Mobile Computing

Staff with laptop computers and other mobile computing devices shall take all sensible and reasonable steps to protect them from damage, loss or theft. Such steps may include:

- Securing laptops and removable media whether in college or while travelling.
- Avoiding taking laptops into areas with a high risk of theft and locking such equipment in the boot of a vehicle when leaving it unattended
- Staff shall ensure that confidential information cannot be viewed by unauthorised persons when using computing equipment in public places (e.g. stations, airports, trains, etc.)
- Use of external wireless access points shall be permitted provided that member of staff ensures that the firewall software provided with the mobile computer is activated. Any sensitive data to be passed over an external wireless access point must be encrypted.

Staff using mobile computers and smart phones are required to ensure that software controls and updates are installed and regularly updated to protect the mobile computers and smart phones from viruses, spyware and similar malicious programmes. Regular updates of anti-malicious software files should occur automatically on connection to the Internet

Use of any mobile computing device owned by the College must be in accordance with this Policy and the relevant section of the Staff Handbook.

Any mobile computing device owned by the College that is stolen or lost MUST be reported to the IT Officer and the Director of Communications immediately, regardless of the time of day or date.

ix. Software Compliance

The College will provide legitimate copies of software to all staff users who need it, and will ensure the necessary authorisation has been obtained.

Members of staff who are users of College computer equipment and software shall not copy software or load unauthorised/unapproved software onto a College computer including mobile equipment. The Director of Communications is responsible for giving authority and approval for software suitable for loading on College equipment and is supported by the IT Officer.

Members of staff shall not give any of the College's software to any outsiders, including senior members/students.

The IT Department shall maintain a register of authorised software, including the licence information. All licences and media shall be held securely in the IT Office.

Licensed software shall be removed from any College-owned computer that is to be disposed of outside of the College.

Further Software Usage Policies are included in the Staff Handbook.

x. Clear Desk/Clear Screen

Outside normal working hours, all confidential information, whether marked up as such or not, shall be secured; this may include within a locked office or in a locked desk. During normal office hours such information shall be concealed or secured if desks are to be left unattended in unlocked/open access offices.

Confidential printed information to be discarded shall be placed in an approved confidential waste container as soon as reasonably practical, or kept secure until that time.

Documents shall be immediately retrieved from printers, photocopiers and fax machines.

All desktop computers shall be logged off or locked automatically after a suitable period (unless required to remain on for operational purposes) to restrict access when the user is not at his or her desk.

Unattended laptop computers, mobile telephones and other portable assets and keys shall be secured e.g. in a locked office, within a lockable desk, or by a lockable cable.

Those in charge of meetings shall ensure that no confidential information is left in the room at the end of the meeting.

The College shall ensure that members of staff have suitable storage facilities to enable them to comply with this Policy.

xi. Information Backup

The requirements for backing-up information shall be defined based upon how often it changes and the ease with which lost data can be recovered and re-entered.

The IT staff shall be responsible for ensuring that systems and information held on the College servers are backed up in accordance with the defined requirements. No systems of information should be held on local hard drives to avoid the risk of this information not being backed up.

Accurate and complete records of the back-up copies shall be produced and maintained.

The back-ups shall be stored in a remote location which must:

- be a sufficient distance to escape any damage from a physical disaster at the College be accessible
- afford an appropriate level of protection to the back-up media in terms of its storage and transportation to and from the remote location

Back-up media shall be regularly tested to ensure that they can be relied upon for emergency use when necessary. Restoration procedures shall be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.

xii. Data Breach/Loss

Data breach policies shall be in place to handle loss of data. Such breaches shall include any breaches of this policy. Breaches include but are not limited to:

- data breach/loss/theft
- loss of equipment due to theft
- inappropriate access controls allowing unauthorised access
- equipment failure
- human error
- unforeseen circumstances such as fire and flood

- hacking
- ‘blagging’ offences where data is obtained by deception.

Any breach should be immediately reported to the Director of Communication and the IT department who services the College, and to the appropriate head of department. All investigations should be carried out urgently and reviewed once the issue has been resolved. Responsibility for the reporting of any data breach is up to the information owner, and where it contravenes GDPR and DPA must be reported to the Office of the Office of the Information Commissioner by the Data Protection Lead or the Director of Communications or the person who first notices that a breach has occurred.

9. Disposal

Policies and procedures must be in place for the secure disposal/destruction of confidential information. The College complies with national guidance from the National Cyber Security Centre: Secure sanitisation of storage media - NCSC.GOV.UK All information held on computers and storage devices will be sanitised prior to disposal in compliance with the Data Protection Act 1998..

10. Governance

This Policy will be reviewed regularly by the Data Protection Lead. Any changes will be approved by the Governing Body.

Appendix 1

Data Systems Location/’Owner’

Payroll	Accounts Team
Accounts	Accounts Team
Admissions	Registry
Alumni	Student Services
Book Cataloguing and Usage	Libraries
Archive Records	Archivist
Accommodation/Buildings	Director of Facilities and Building Managers
Security	Director of Facilities
Networks and IT systems	IT Office
Personnel	HR Manager
Website	Director of Communications and IT Support. Programme Managers and Director of Quality
Legal agreements and Deeds	Board of Directors
Governing Body & committee minutes & agendas	Secretary to the Board and Director of Funded Programmes