Physical Security Policy

Policy Purpose

The College is responsible for and committed to protecting, as far as is reasonably practicable, the health, safety and welfare of all staff in its employ, in addition to customers, associate faculty, contractors and visitors in, or in the direct vicinity of, its centres.

The College is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems. Additionally, all users interacting with information assets have a shared responsibility to ensure the security of those assets and should assist the College in applying this policy.

The purpose of this policy is to provide a framework and procedures for identifying and dealing with security risk in order to, as far as is reasonably practicable, ensure the safety and security of people, property, data and premises.

This policy articulates the College security as a three-tiered system. Firstly, a culture that is led by security, where people are valued for reporting breaches and protecting the College; secondly through an architecture of security that draws effective perimeters around people, property, data and premises; and thirdly, through adequate systems to protect staff and data, should a physical breach occur or should a cyber-attack be attempted remotely.

The College must have controls in place to ensure the smooth operation of the IT Resources. Users must be trained, equipped and periodically reminded to use information and associated infrastructure securely. There must be secure procedures in place for how equipment and hard copies of data is acquired, stored, redeployed and disposed.

This policy seeks to encourage adaptability: vulnerabilities or breaches will be reported, assessed and reviewed and recommendations made for improvement plans. The College provision of physical security should be built on regular risk assessment, which will review how security can be built and maintained through physical barriers, data strategies and a shared culture.

Legislation and Standards

This policy is informed by the following:

The Health and Safety at Work etc. Act (1974)
The Occupiers' Liability Act (1984)
The Regulatory Reform (Fire Safety) Order (2005)

Responsibilities

The Board:

- Must take ultimate ownership of security risk
- Is responsible for implementing clear policy, procedures and reporting lines for security

Facilities Manager:

- Should coordinate with the Chief Operating Officer to establish clear and regular links for how physical, personnel and cyber security is managed within the College
- Should coordinate with the Chief Operating Officer to ensure that adequate training programmes are available for all staff and students, so that those on site are able to recognise and respond to any breach
- Should arrange additional training to responsible persons, so that the College can be safely evacuated in an emergency
- Should produce security risk assessments for centres under their control
- Should ensure adequate measures on in place for maintaining the efficiency of access control systems – e.g. by changing access codes regularly (monthly for all staff areas, and every quarter for student areas) and/or whenever there is significant change to the student population or level of risk.

Chief Operating Officer:

- Should coordinate with Facilities to establish clear and regular links for how physical, personnel and cyber security is managed within the College
- Should coordinate with the Facilities Manager to ensure that adequate training programmes are available for all staff and students, so that those on site are able to recognise and respond to any breach.
- Should advise on matters relating to the storage of CCTV data, biometric data, and health data gathered in the process of making systems accessible for all users
- Should advise on the impact of statutory regulation

Health, Safety and Environmental Lead:

- Should maintain policy, and review it annually (or after significant change to the College or its operations)
- Should advise on the impact of statutory regulation

Information Owners:

- Must support Line Managers to ensure appropriate physical controls are in place to establish secure areas, and developing suitable and sufficient risk assessments

Academic Staff and Line Managers:

- Should ensure that their staff and students are familiar with the security procedures for their location, and have attended all necessary training

- Should complete a lone worker risk assessment for all direct reports who fall into this

category
- Should ensure that home workers under their leadership subscribe to College-wide security measures

All Employees and Students:
- Should put measures in place to ensure those who supply, operate and maintain systems – both physical and digital -- are reputable and reliable
- Should not misuse any equipment that is provided for security purposes (e.g. by propping open a coded door)
- Should follow instructions from the College on security matters and attend relevant training
- Should report hazards and defects observed in the workplace
- Must act in accordance with the training, signage and guidelines provided
- Must cooperate with the College by following security protocol, wearing the required identification, reporting unauthorized or otherwise suspicious activity and communicating potential threats to responsible person(s)
- Must immediately report the loss, theft or breach of items that should be secure (e.g. laptops), or items provided for the purposes of security (e.g. security passes)
- Must, on joining the College, coordinate with HR to obtain official identification (e.g. a lanyard and security pass)

Site Visitors and Contractors

The following control measures are in place to maintain levels of security when a contractor enters a site or system:
- Measures must be in place to ensure all contractors are reputable and reliable
- All contractors on site must provide documentation and references
- The perimeters of the visit/work must be clearly defined and articulated
- Secure information should only be shared if it is lawful to do so under GDPR, and if it is necessary to for the completion of the task
- Risk assessments must be carried out by the College before works start to ensure that any risks to the contractors or the College employees and visitors are addressed.
- The contractor must report to their on-site contact at the College, before starting work
- Contractors must be advised of the College's Fire Evacuation and First Aid procedures.
- All contractors must sign in and out of the building and wear visible identification.
- Contractors should be monitored during works to ensure that they are following H&S and Security procedures.

Physical and Environmental Security procedure

To prevent harm to people and unauthorised physical access, damage and interference to the College's information and assets.

Physical Security Perimeter

The College information processing facilities and equipment must be protected by a physical security

perimeter. This includes equipment used for the processing of data off site (e.g. within home offices).

Sensitive information and assets must be protected while considering the safety of personnel.

The following controls must be applied, with regard to physical security perimeters:

- Security perimeters must be clearly defined by the Facilities Manager using the template available, and the siting and strength of each of the perimeters must depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
- Perimeters of a building or site containing information processing facilities must be physically sound (i.e. there must be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site must be of solid construction and all external doors must be suitably protected against unauthorised access with control mechanisms, e.g. bars, alarms, locks, etc.; doors and windows must be locked when unattended and external protection must be considered for windows, particularly those at ground level, adjacent to drainpipes or near flat roofs;
- Special consideration must be given towards physical access security when the facility houses multiple organisations or COllege units (for example, when the College is a tenant of a building occupied by numerous businesses and/or visitors, keypad access should be in place to secure the College's offices)
- All alarm system must be checked over and serviced by an approved company every year;
- A manned reception area or other means to control physical access to the site or building must be in place at the main entry point to the College; access to sites and buildings must be restricted to authorised personnel only;
- Physical barriers must, where applicable, be built to prevent unauthorised physical access and environmental contamination; attention should be paid to weak spots (e.g. through defensive planting) or points of disrepair (e.g. broken fence);
- Access points to premises should be kept to a minimum, to facilitate greater control
- All fire doors on a security perimeter must be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national, and international standards;
- Suitable intruder detection systems must be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas must be alarmed at all times; cover must also be provided for other areas, e.g. computer room or communications rooms;
- In order to deter intruders, obscured areas around each location should be kept to a minimum (trim trees, shrubs and undergrowth to open up the view);
- Security lighting should be installed, whenever recommended through a risk assessment
- A security risk assessment should be integral to every refurbishment project that impacts a defined security perimeter;
- Security measures for newly built or acquired premises must be in place from the outset;
- Outbuildings must be secured, so their location or contents do not compromise location security;
- Adequate lighting should be provided in and around the College buildings;
- Items requiring additional security should be stored out of view, when not in use.
- A secure area may be a lockable office, or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may

be needed between areas with different security requirements inside the security perimeter.

- When additional security measures are taken to secure the building and if doors are to be secured using extra locks or padlocks there must be a strict management procedure in place for removal of these, this must be a written procedure and must be fail safe.
- In accordance with the Group Health and Safety Policy and the Occupiers' Liability Act (1984), no security measure should compromise the safety of those on the property, regardless of whether their presence is lawful or not.

Physical Entry Controls

Secure areas must be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. The following controls must be implemented:

- Access to areas where sensitive information is processed or stored must be restricted to authorised personnel only;
- Authentication controls must be used to authorise and validate such access;
- Visitors must be escorted by authorised personnel; staff must collect visitors from reception
- Visitors must only be allowed access for specific and authorised purposes;
- The date and time of entry and departure of visitors must be recorded using a visitors' book displayed at the College reception of each building;
- All employees and other authorised personnel must wear visible identification;
- Visitors must be issued badges or tags of a different colour than employees;
- Employees must notify the Facilities Team when they encounter unescorted visitors or anyone not wearing visible identification;
- Third-party support personnel may be granted restricted access only when required; their access must be authorised and monitored; e.g. contractors
- Access rights must be regularly reviewed by the Facilities team at each site.
- Codes to student areas should be changed regularly, reflecting the change to the authorised population;
- Safeguards should be in place to prevent tailgating.

Securing Offices, Rooms and Facilities

Controls to ensure security of information and information systems located in the College offices, rooms and other facilities must be designed, applied and documented.

The Facilities Manager must regularly assess the security of areas where sensitive information is processed and/or stored.

Controls that may be implemented to reduce associated risks are:

- Physical entry controls
- Proper storage for sensitive information, when not in use
- Ensuring directories that identify the locations of data centres and other areas where sensitive information are not public

Closed Circuit Television (CCTV)

The College uses closed circuit television (CCTV) across its centres. CCTV on site serves as part of an overall security package, in conjunction with a monitored alarm, security personnel and/or staff vigilance. Please refer to the College's CCTV Policy for further details.

Protecting Against External and Environmental Threats

Physical protection against natural disasters, malicious attack or accidents must be designed and applied.

Fire safety legislation places a requirement on Employers to carry out a fire risk assessment of their workplace. Such assessments should be mindful of the potential security threat.

Information Owners, Data Center Managers, IT Security staff, planners and architects must incorporate – to the extent possible – physical security controls that protect against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural and man-made disaster. Consideration must be given to any security threats presented by neighbouring premises or streets. In addition to building code and fire regulations:

- Combustible or hazardous materials must be stored at a safe distance from the secure area;
- Bulk supplies, e.g. stationery, must not be stored in a secure area;
- Backup equipment and backup media must be located at a safe distance to avoid damage from a disaster affecting the main site; and
- Environmental alarm systems, fire suppression and firefighting systems must be installed

Delivery and Loading Areas

Access points such as reception, delivery and loading areas and other points where unauthorised persons may enter the premises must be controlled and, if possible, isolated from secure areas or offices to avoid unauthorised access.

Measures must be in place to review mail-handling procedures, so that any security or safety risks can be identified and mitigated.

The Facilities Manager must ensure that:

- Access to a delivery and loading area from outside of the building must be restricted to identified and authorised personnel;
- The delivery and loading area must be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;
- The external doors of a delivery and loading area must be secured when the internal doors are opened;
- Loading docks and delivery areas must be regularly inspected and actively monitored;
- Incoming material must be registered in accordance with asset management procedures on entry to the site and booked in with the Facilities team.

Reporting Security Incidents

Procedures must be in place for responding to and reporting a security breach, and collecting documentation so as to identify what may be compromised, and to develop more robust defenses.

All crimes, unauthorized access and suspicious activity should be documented and reported to the Facilities Team, following incident-reporting procedures and using an incident form.

All monitored alarms MUST have at least two nominated key-holders who can be contacted if the alarm is activated whilst the premises are unoccupied.

Business continuity

The College has a business continuity plan that is regularly reviewed, and improved as appropriate, so that the College is equipped to continue with minimal interruptions, in the event of any incident.

Security is a core element of this plan; the business continuity plan is reviewed in dialogue with the College's security risk assessments.

1. Document Controls

1.1. Document Approvals

Named person(s) below indicates that this document has been reviewed and approved by the appropriate people. This document is subject to formal change control procedure.

Date	Role/Position	Name
08/12/20	Chief Operating Officer	Matt Green
18/06/24	Chief Executive Officer	Christina Cunliffe

1.2. Amendment History

Date	Version	Author	Description
18/06/24	6.0	Matt Green	Minor changes