Building Access Control Policy

Purpose

As an employer the College will ensure, as far as is reasonably practical, the personal safety and security of all staff, students and visitors whilst on College premises.

As an educational establishment, the College promotes an open access policy which is an essential part of an academic life. Some security measures are therefore necessary to maintain a safe and secure environment for our staff, students and visitors. These measures will vary depending on location and site function.

To ensure the security of staff and students, each College site will develop and apply controls and procedures which will be appropriate and reasonably practicable for the scale and type of potential risks and hazards present in the area where the site is located. An access control risk assessment will help determine the right level of access control measures.

Scope

This policy describes the general building Access Control System (ACS) at the College. The policy relates to both PC-based and stand-alone keypads. This ensures that access control measures do not act as hindrance to learning activities but are necessary for the safe and efficient operation of the college.

Responsibilities

The following stakeholders are responsible for the management and operation of building access control.

All staff, students and visitors:

- Should share responsibility for security. Everyone must report all criminal activity, suspected or real, or any suspicious activity to reception or to the College Health, Safety and Environmental Lead.
- Should follow the procedures in this Policy. Staff should pay particular attention to those issues which are relevant to their activities.

The Principal and Executive Team should:

- Hold primary accountability for the access control system;
- Ensure that support and resources are available for the implementation of the Policy;
- Ensure resources are available to maintain access control measures;
- Allocate Access Control in a way that is suitable to the business and other policies,
- Manage problem resolution and arbitration.

Managers should:

- Promote security within their area and ensure their staff and students are familiar with their local access control procedure;
- Ensure that members of staff and students in their department/faculty understand and exercise their security responsibilities;
- Orchestrate the overall development and planning of access control procedures for their sites;
- Monitor these policies and procedures to ensure their continued effectiveness;
- Support in the investigation of serious crime and breaches in security;
- Liaise with police, emergency services and local authorities.
- Unlock all perimeters of their building at the beginning of each day, and lock all perimeters at the close of each day;
- Conduct day-to-day management and implementation of the access control policy and procedures;
- Conduct day-to-day monitoring of access to the buildings;
- Provide on-going assistance on matters relating to building and room access;
- Respond to intrusion alarms and other disturbances;

Academic Staff:

- Should ensure that their staff and students are familiar with the access control procedures for their location.

Access Control

The access control procedure for each College location must address the needs of the site, staff and students.

The appropriate level of access control will be determined by the Facilities Manager, and with consideration of the site access control risk assessment.

Arrangements

All buildings will have access control via a stand-alone Keypad.

PC Access Control Systems will be interfaced into the building/Landlords' Fire Alarm System, where fitted. In the event of a fire alarm condition, the ACS Software will command all doors controlled to release. A Green Break Glass Module will be installed to each door as a secondary form of over-ride.

Authorised Individuals

Access to areas where sensitive information is processed or stored must be restricted to authorised personnel only.

All employees and other authorised personnel must carry security key fobs at all times while on site in accordance with the following:

- Security key fobs should be closely controlled, and not leant or transferred to another individual
- Visitors must be issued visitor badge lanyards
- Visitor badge lanywards remain the property of the College. Their loss or theft must be reported at the earliest opportunity, and they must be handed back to the to the reception team or when a user is no longer authorised to access the College premises
- Visitors must be escorted by authorised personnel
- Secutiry key fobs remain the property of the College. Their loss or theft must be reported at the earliest opportunity, and they must be handed back to the to their Line Manager when a user is no longer authorised to access the College premises
- Staff must collect visitors from reception
- Visitors must only be allowed access for specific and authorised purposes and will be monitored
- 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
- 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;
- Safeguards should be in place to prevent tailgating
- Training should be in place to equip staff to challenge strangers

Coded Door lock system

Coded door locks operate in many areas and locations. Coded door locks allow various levels of access and increase security of premises.

Access codes are provided to staff upon joining the College in accordance with the following:

- The College students receive access codes on arrival or via email
- Access codes should be changed at a minimum of monthly for all staff areas, and every quarter for student areas
- In the event of a staff exit as a result of disciplinary action, redundancy or other context involving potential ill-feeling, codes should be changed the day they leave the business or at the earliest opportunity
- Similarly, should a member of staff take garden leave due to their seniority or access to confidential or business-critical information, the codes should be changed immediately
- Visitors and contractors are to be chaperoned by hosts with the exception of regular contractors who will be provided with the code upon their first arrival. All contractors and visitors should sign in at reception
- The responsibility for visitors and their access to premises will lie with the hosts. Visitors must be supervised and chaperoned by their hosts at all times.

Access Control System Keypads

The height of readers and keypads, use of prominent signage, entry/exit times, and emergency

procedures must be considered in the development of the access control system.

In order to ensure readers are accessible to all Code users, as far as possible the access control system will:

- Use a consistent user interface for all key pads
- Identify key pads with appropriate signage
- Place key pads at the same height and position to enable a blind person to locate readers reliably
- Position the key pad at a height which can be conveniently reached by all Code users

Access Control Risk Assessment

The level of access control is based on risk assessment and individual site needs and will subsequently define the appropriate level of control measures.

Factors which must be considered in developing access control measures shall include:

- Location of the site
- Previous history of security breaches
- Site opening hours, number of reception staff working on reception desk
- Expensive devices, equipment or other property that could be targeted for theft
- Staff areas that should have restricted access by College staff only
- Equipment of which use must be restricted to authorised / trained users
- Any activities that should not be disturbed (e.g. exams)

USE OF CLOSED CIRCUIT TELEVISION (CCTV)

The College facilities team control CCTV systems. Please refer to the College CCTV Policy for further information.

BUILDING OPENING HOURS

Standard access times will apply to all buildings as notified in writing from time to time.

Normal opening hours

Standard opening hours vary from site to site. During opening hours

- Entry and exit is controlled via a Card/Code
- Day visitors are issued with a reusable visitor card from a controlled set reserved for the purpose

Areas not normally accessible by the public may have other restrictions during these hours.

Outside normal opening hours

- Most buildings are locked down to a single entry/exit (with the exception of emergency exits)
- Entry is via an authorised Card/Code
- Egress is via a Card/Code as applicable

ALARM REPORTING

A warning alarm will notify the Facilities Team of any of the following conditions:

- invalid attempts to access/egress a building
- forced door
- use of an emergency exit switch

LIABILITY

The College does not assume responsibility for any lost or stolen personal property on its premises. Personal valuables should be locked away or placed out of sight or kept on the person, and personal property should never be left unattended. If a theft occurs, it should be reported to a Line Manager or reception immediately.

Access for people with disabilities

The Access Control System will take into account the requirements of code users with disabilities. Access Control System development will follow the College's Equality, Diversity and Inclusion Policy.

Any preferences specified by disabled users will only be made available to authorised staff in accordance with the General Data Protection Regulations (GDPR). In particular, information relating to an individual's health will usually constitute sensitive personal data under the GDPR and will therefore be subject to additional processing safeguards.

If a disabled user has any issues or suggestions relating to the Access Control System, they should contact the Facilities Team.

EMERGENCY PROCEDURE

The procedure to be followed should be described in the Code user's PEEP (personal emergency escape plan), and agreed with the Health, Safety and Environmental Lead and Security Services.

Emergency Evacuation

In the event of a fire or other threat, this policy covers all eventualities by utilising fire/evacuation wardens sweeping the building to ensure it is clear of staff, students, visitors and patients, as well as a registration system that is checked to ensure all are accounted for. The process is set in motion by the activation of the fire alarm either from the wall mounted call points or triggered by the smoke detection system. Smoke control doors on the ground floor are automatically triggered to close and the entry/egress security doors automatically default to unlocked.

The external evacuation point is sign posted at the rear of the building and the procedure requires regular evacuation exercises to ensure a speedy and familiar response. Fire wardens are trained to sweep designated areas of the building moving from the centre to the exterior collection point.
Modesty gowns are located in the patient clinics to ensure immediate evacuation. Building layout diagrams are located at all the entry/exit points to aid the fire department in the event of fire. The fire alarm sounding system is tested weekly.

Business continuity

The Facilities Team will liaise with the ACS service provider and building management to resolve ACS system failures.

A regular review of business continuity issues, between the stakeholders, should take place at least quarterly so that improvements can be fed back into system management.

Information management will provide reports on the ACS to the Facilities Team:

- ACS management system issues and down-time
- Application and database support time and activity

The following describes potential business continuity problems and the likely impact:

Network or server related

In respect of PC Based Access Control, the local (building) controllers retain sufficient Card user information to enable access/egress during a network or server outage. New or updated Card user information however, will not be available during this period.

Power failure

In respect of PC Based Access Control, the building access control will continue to function during a loss of building power via a landlord managed emergency generatior.

Complete failure

During a period of complete power failure (where battery power has been exhausted), or the controller has malfunctioned, or doors are either in a fail secure or fail open situation as applicable, manual inspection of identity cards may be required for buildings access control. This will be co-ordinated via the building management.

Normal opening hours

If complete failure occurs within normal opening hours, all buildings, with the exception of high-risk buildings, fail open and the rest will fail secure.

Outside normal opening hours

Based upon the building risk category, outside normal opening hours, most building access points will fail secure. All doors also have an emergency (break glass) override to manually open the door as a secondary safety feature. Where an emergency override is not installed an emergency call number will be provided to contact the building management.

Incident Reporting

In order to prevent any security incidents and to raise awareness all staff, students and visitors should:

- Report all incidents of crime on College premises, real and suspected

- Report all suspicious activity to the Facilities Team Leaders or reception immediately

Incident reporting allows investigation and recommendations to be made to prevent a recurrence and to ensure that adequate resources are provided to prevent such incidents. Theft on premises should also be reported to the local police.

Criminal Offences committed by staff, students or visitors will be reported to the Police. In addition to any police involvement into criminal offences by staff, the HR Lead will be informed in order to assess and determine whether any disciplinary action should be taken under the College Disciplinary Procedure.

Incidents Investigation

All access control incidents and crime that take place on College premises will be investigated appropriately to prevent re-occurrence.

- An investigation team will be put together to investigate a reported incident
- The size of the team and persons involved into the investigation should be appropriate for the severity of an incident. For example, for low risk minor incidents, an investigation by the HSO might be sufficient. For higher risk incidents, members of the Executive Team will be involved.

Information Management

Data Protection:

- Personal data will be processesd in accordance with the GDPR
- AC system managers and administrative staff will ensure that AC data is only used for its intended purpose
- Personal usage information will not be extracted from the ACS or shared with other Group systems without the explicit consent of the Chief Operating Officer or their representative
- Unless specifically requested, for legislative or academic reasons, personal usage data will be removed from the system after 90 days
- Access preferences, for disabled users, may only be made available to an authorised member of College staff
- Information relating to an individual's health will usually constitute Sensitive Personal Data under the GDPR and will therefore be subject to additional safeguards when processed

Personal access reports:

- Personal access information will not routinely be divulged to any third parties. Typical reasons for requesting this information may include; a disciplinary investigation; after a crime has occurred or because of health and safety concerns. If approved, the Chief Operating Officer will inform the Facilities Team to release the requested information to the enquirer
- Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act and the GDPR

- All requests should be made in writing to the Data Protection Officer
- Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified
- The College must respond to a request within one month of receiving it
- The College reserves the right to refuse access to security data where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.
- In an emergency the College may also make use of personal access reports, as part of its crime prevention and safety role
- Personal access information held on a PC will not be divulged to third parties unless the cardholder is the subject to a written request by a relevant external agency (e.g. the police) in line with the GDPR

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
18/01/21	Chief Executive Officer	Christina Cunliffe
18/06/24	Chief Executive Officer	Christina Cunliffe

1.2. Amendment History

Date	Version	Author	Description
18/06/24	2.0	Matt Green	Minor changes