**ED-65**





**Queen’s University Belfast**

Control of access to buildings

policy and procedures

Estates Directorate

**Overview**

The physical access to most University buildings is controlled centrally by Estates Security. This Policy and Procedure provides details on how access can be granted to individuals, it applies to Staff, Students, Contractors, Additional Persons and Visitors on official University Business.

Developed by Estates Directorate

11 May 2016

**Contents**

|  |  |
| --- | --- |
| Reference | ED-65-001 |
| Date approved | 11 May 2016 |
| Approving Body | Health & Safety Management Group |
| Implementation date | 11 May 2016 |
| Version | 2016/001 |
| Supersedes | N/A |
| Consultation undertaken | Health & Safety Compliance Committee and Health & Safety Review Group |
| Target audience | All Students, Staff and Contractors |
| Supporting Procedure(s) | Included |
| Review Date | May 2018 |
| Author | Head of Administration & Resources (Estates Directorate) |
| Responsible Managers | Directors, Directors of Operation, Pro-Vice-Chancellors, Heads of Service |
| Competent Person (if applicable) | N/A |
| Duty Holder (if applicable) | N/A |
| Further Guidance/Information | Head of Administration & Resources (Estates Directorate) |

# 1. Policy

* 1. Rationale

The University has over 1500 access controlled doors across the campus. Whilst the majority of Schools and Directorates provide open access during normal working hours and study periods, some do allow staff and students access to buildings outside these hours. In the interests of security and safety, it is important that a Control of Access to Buildings Policy and Procedures are in place to provide a clear framework and operational guide.

* 1. Objectives

The objectives of this policy and associated procedures are to:

* Provide building access to all authorised staff, students, contractors and individuals under the class of ‘Additional Persons’
* Provide accurate information on control of access to buildings across the University
* Provide procedural information for all users of the system
* Circulate and update procedural documentation as required
* Within the overall objective of providing an open accessible campus, ensure that realistic and deliverable security is provided where necessary.
  1. Policy Statement

To meet the objectives of this policy, the University will ensure effective systems and procedures are in place to deal with the control of access to buildings, recognising the importance they have in student and staff security and safety. To enhance identification of staff and recognised contractors corporate staff ID badges must be worn prominently at all times in work (except when this presents a safety hazard) or carried on person and be displayed upon request.

1.4 Responsibilities

This policy and associated procedures are applicable to the following personnel:

* All students, staff and visitors to the University – User awareness
* Schools and Directorate nominated staff – manage student, staff and additional persons access. These individuals are the end-users of the system. Generally staff cannot apply for access through an on-line facility.
* Security Control Room Staff – Daily operational management
* Estates IT Support Group – Resolve escalated issues and provide full database management on the Hirsch Velocity system. In addition, manage the Queen’s Online Request System.
* Schools, Directorates and Faculties will be responsible for the supply of lanyards and/or other arrangements for the carrying and display of Staff Identity Cards as appropriate.
  1. Consultation

This policy has been consulted with the University Health & Safety Compliance Committee.

* 1. Approval and Review

This policy and supporting procedure has been approved by the Health & Safety Management Group and will be reviewed on an annual basis.

# 2. Procedures

The following procedures are applicable when applying for and granting of access permission to staff, students and visitors.

2.1 Definitions

The following definitions are applicable to the Access Control Policy and Procedures:

|  |  |
| --- | --- |
| Access Control | The process of limiting access to buildings using electronically controlled locking devices. |
| Additional Persons | Individuals who require certain privileges to access University systems and are not staff or students. |
| Authorisers | University staff with approval to grant access to high security areas. Authorisers cannot approve access to high security for areas within the School or Directorate for which they are the Authoriser. This must be approved by the Estates Manager (Security) or his deputy. Appointment to this position is made by a Director or Head of School in writing to Estates IT Support Group. |
| Building Operating Times | Standard opening hours of University buildings. |
| Card and PIN Access | In certain high security areas it may be deemed necessary to increase the level of security applied to an electronically controlled door. This can be achieved by requiring both card and PIN to be used in order to open the door. |
| Card Reader | Each door controlled by the Hirsch Velocity System is accessed by means of a card reading device. These devices can be operated by either an approved smart card or approved PIN code |
| End-Users | End-users are the nominated staff in the School or Directorate who make changes and requests to the access control system. |
| Estates ITSG | The Estates Directorate’s Information Technology Support Group. |
| High Security Areas | Areas within the University where access has been restricted and can only be granted by designated authorisers |
| Hirsch Velocity System | The electronic system controlling access to buildings using a combination of magnetic or electro-mechanical locks. |
| Hotlisting | The process whereby access is terminated/suspended. PIN codes and card access is withdrawn. |
| Pathways | A designated course of study leading to a qualification from the University. In the context of access control the Pathway informs the system of the minimum access requirement for students on this pathway as determined by their School. |
| Private Access | The process whereby Requestors/Authorisers provide access to buildings to staff/students/additional persons which exceeds the basic pathway or standard opening times. |
| PIN Code | Each user assigned access to any University building is provided with a unique code that provides access to assigned areas. |
| Queen’s Online Access Request System | The interface provided to University staff to allow granting of access or application for access to virtual buildings including high security areas. |
| Requestors | University staff with approval to request access through Queen’s Online for staff, students and additional persons associated with their School or Directorate. |
| Security Control Room | Security can be contacted on  5099 – for access issues and general security advice  2222 – in an emergency |
| Smart Card | The staff, student or additional person card provided by the University. |
| Time Zones | Access to buildings outside their normal opening times for each individual is restricted to one of four time periods known as Time Zones.  The available Times Zones are:   |  |  | | --- | --- | | Monday to Friday | 07:00 to 19:00 | | Monday to Friday | 07:00 to 23:00 | | Monday to Sunday | 07:00 to 24:00 | | Monday to Sunday | 00:00 to 24:00 (24 hours) | |  |  | |
| Virtual Buildings | Access to the University buildings is created using a series of Virtual Buildings. These Virtual Buildings allow each building to be sub-divided, if required, into smaller units to provide the required level of access management. |

2.2 Background

Access to University buildings outside their normal opening times is controlled by two distinct computerised options. The request to provide access is managed using the Queen’s Online Access Request system while the functioning of the physical door access is controlled using the Hirsch Velocity system. Both these solutions are managed by the University Estates Directorate.

End Users are granted privileges on the Queen’s Online system to request access for new staff, students and additional persons as well as being able to manage existing requests. This system is used to populate the Hirsch Velocity System on a daily basis providing the requested access. In addition, the Queen’s Online system monitors the Staff, Student and Additional Persons databases to ensure only current staff, students and additional persons are permitted access to the University. Some areas are designated High Security and these have special restrictions applied. The Security Manager, in consultation with the Safety Service, if necessary, will advise and ultimately approve whether an area should be high security. The following sections provide details on how access can be obtained/granted for students, staff, additional persons together with contractors and visitors working in the University on official business.

Appendix 1 provides information on key tasks and responsibilities. Appendix 2 illustrates the process diagrammatically in a flowchart.

2.3 Student Access

2.3.1 Pathways

School requestors can add/delete/modify access privileges to a Pathway using the QOL Access Control System based on the Virtual Building to be accessed and the selected time zone for this access. The requestor can only request access to Virtual Buildings that they are nominated to request.

Access can be granted to a specific year of the Pathway or it can be granted for the duration of the Pathway. When access is added to the student Pathway all students who register on this Pathway will automatically be granted the access assigned. For new students the access will be added to the new student card and an email will be sent to the student providing them with a pin code which will also operate the doors allocated. For existing students the access will be added to the card only. No email will be sent since each user will have previously been issued with their pin code.

Access privileges assigned in this manner are valid for the duration of the student participation on the Pathway. Students who have completed their course, have changed Pathways or have left the University will have their access privileges removed automatically.

At the end of each academic year students are expected to re-register for their course. Any student who fails to re-register for their course will have their access privileges removed.

Please note that using this method will grant the same access to all students enrolled on the specific Pathway.

2.3.2 Clusters

Some Schools operate on the principle of Research Cluster rather than the concept of Pathways. Although the process is the same as for the pathway method, in this instance the required access is granted to the cluster managed by a supervisor. Any student assigned to the supervisor will be automatically granted the required access privileges. As in the case of Pathways, if a student leaves the cluster or fails to re-register all granted privileges will be automatically revoked.

Please note that using this method will grant the same access to all students enrolled on the specific cluster.

2.3.3 Private Access

Although access can be granted to students using the Pathway or Cluster option it is possible to provide additional specific or private access to individual students. If an individual student requires specific access the private access option allows requestors to assign the correct access level. In private access the access requested can be granted to the individual for the duration of their course or for specific dates.

If a student has already been granted access using the Pathway or cluster method it is not possible to grant them specific access to the same Virtual Building assigned to the Pathway or cluster even if it is for a different time zone.

2.3.4 High Security Access

In certain circumstances it is necessary to assign high security requirements to access privileges. In these circumstances any request for student access to these areas must be approved by an Access Control Authorised person on an individual student basis. The methods described previously for granting student access are still applicable but it should be borne in mind that granting access to a high security area using the Pathway or cluster method will require individual approval for each student before the access requested will be assigned to their smartcard.

2.4 Staff

2.4.1 Private Access

School or Directorate requestors can add/delete/modify access privileges for any member of staff assigned to their School or Directorate but, only when the staff member has been allocated a space location in the QOL Access Control System. The requestor can only request access to Virtual Buildings that they are nominated to request.

Access to staff using this method can be granted for the duration of the staff employment or for specific dates as required. Once requested, access for new staff members, will be automatically added to the new staff card and an email will be sent to the individual providing them with a pin code, which will also operate the doors allocated. For existing staff members the access will be added to the card only. No email will be sent since each user will have previously been issued with their pin code.

Please note that, if a member of staff is moving to a different School or Directorate, the Requestor must ensure that any privileges issued to the individual are removed before the changeover occurs. They will be unable to remove the access after this date because they will have no further access to the staff record when the move has been completed in the Human Resources system.

2.4.2 High Security Areas

In certain circumstances it is necessary to assign high security requirements to access privileges. In these circumstances any request for staff access to these areas must be approved by an Access Control Authorised person on an individual staff member basis. Access to High Security areas is requested in the same way as any other request for access.

2.5 Additional Persons

2.5.1 Access can be granted to University buildings for new additional persons however in this instance no smart card will be available and access to the requested buildings will not be made available until an Additional Persons smart card is produced by Estates ITSG. School or Directorate staff must ensure that an appropriate digital photograph is sent to [estates.systems@qub.ac.uk](mailto:estates.systems@qub.ac.uk) to allow the issue of the required smart card. This photograph must be accompanied by the associated Additional Persons number. Cards will only be issued for Additional Persons who have an outstanding request for access on the QOL Access Control System.

For Additional Persons with a valid smart card the School or Directorate Requestor can request the required access to University buildings. The access granted is time specific for an Additional Person and the Requestor must enter the start and end date for each request. The remainder of the procedure is the same for staff private access with the exception that no location information is required.

2.6 Manual Access to Buildings

All manual access to buildings is centrally controlled and monitored by the University Security Service.  All enquiries regarding manual access to University buildings should be directed to the Security Control Room on 028 9097 5098/99.

2.6.1 Mechanical Keyless Push Button Locks

All Schools and Directorates must consult with the Assistant Estates Manager (Security) – Tel No. 028 9097 5005, on the installation of any mechanical keyless push button locks.

This is important and will ensure the following:

* Any Emergency Service response will have the correct information to gain access to all areas across the University.
* The lock is compliant with current regulations and standards
* The location of the lock can be recorded centrally by the Security Control Room
* The pin code can be confirmed, recorded and centrally held by the Security Control Room

2.7 Unauthorised Individuals on University Premises

If a member of staff has any concern whatsoever about any individual’s authorisation to be within the University premises, they should not challenge the individual, but instead immediately withdraw to a safe area and contact Security Control on ext 5098/99.

2.8 Summary

The foregoing Policy and Procedures have been approved by the Health and Safety Management Group and are applicable to all staff, students, and visitors on University business, contractors and Additional Persons.

**Appendix 1**

# **Key Tasks, Responsibilities and**

# **Steps for Control of Access to Buildings**

| **Task** | **Responsible Group** | **Process Steps** |
| --- | --- | --- |
| Appoint Requestors and Authorisers | Head of School / Directors | Provide staff details to include specific high security access areas for Requestors and Authorisers. |
| Update Requestor and Authoriser details | Estates ITSG | Provide Requestor and Authoriser access to Queen’s Online. |
| Update Users access | Requestors | Update User access requirements on the Queen’s Online Access Control system. This update must include the time period required for each access area. |
| Approve access to High Security areas | Authorisers | Approve or reject request for user access in specific High Security areas. |
| Provide initial contact to users on access issues | Security | Investigate issue for user. If the problem cannot be resolved escalate to Estates ITSG. |
| Manage opening and closing times of individual doors | Security | Update opening and closing times of buildings and rooms as agreed with Schools, Directorates and Room Bookings staff. |
| Remove access to users on request of School or Directorate | Head of School / Directors | Remove access request on Queen’s On Line Access Control System. |
| Report loss of smart card | User | User to inform Security on ext 5099 then contact HR or QSIS to arrange replacement card.  Security inform Estates ITSG and access disabled until new card issued.  Cards suspended using Queen’s On Line will not remove access permissions. It is important to inform Security as above. |
| Emergency request by School or Directorate to immediately remove user access | Security Manager or appointed deputy | Hotlist smart card. |

|  |  |  |
| --- | --- | --- |
| **Contacts** | **Extension** | **Email** |
| Security Control | 5098 / 5099 | security@qub.ac.uk |
| Estates Information Technology Support Group (ITSG) | 5005 | estates.systems@qub.ac.uk |
| Security Manager | 5005 | d.curley@qub.ac.uk |
| Assistant Security Manager | 5005 | r.sheridan@qub.ac.uk |

**Appendix 2**

# **Access Control Flow Chart**

