Electronic Security Systems
Technical Specification & Design Guidance
Document
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>2.0</td>
<td>Purpose of document</td>
<td>4</td>
</tr>
<tr>
<td>3.0</td>
<td>Design process, installation and commissioning</td>
<td>4</td>
</tr>
<tr>
<td>4.0</td>
<td>Principles of deployment</td>
<td>5</td>
</tr>
<tr>
<td>4.1</td>
<td>Electronic access control</td>
<td>6</td>
</tr>
<tr>
<td>4.2</td>
<td>Alarm monitoring</td>
<td>7</td>
</tr>
<tr>
<td>4.3</td>
<td>Surveillance cameras</td>
<td>7</td>
</tr>
<tr>
<td>4.4</td>
<td>Intercom/door entry systems</td>
<td>9</td>
</tr>
<tr>
<td>5.0</td>
<td>Technical specifications</td>
<td>10</td>
</tr>
<tr>
<td>5.1</td>
<td>Access control and alarm monitoring</td>
<td>10</td>
</tr>
<tr>
<td>5.2</td>
<td>Surveillance cameras</td>
<td>16</td>
</tr>
<tr>
<td>5.3</td>
<td>Intercom/door entry system</td>
<td>17</td>
</tr>
<tr>
<td>Appendix A</td>
<td>Security System Specialist Contractor</td>
<td>19</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Gallagher system architecture schematic</td>
<td>20</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Approved lock types</td>
<td>21</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Miscellaneous specification details</td>
<td>23</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Contact details</td>
<td>24</td>
</tr>
</tbody>
</table>
1.0 Introduction

UCL Security’s objective is to use systems and staffing arrangements to help us provide a safe and secure working environment for UCL staff, students and visitors. The UCL Security department is responsible for the policies and procedures that define our approach and our response to security concerns. UCL Security is responsible for the provision of building attendants and security personnel; and the specification, on-going management, support and maintenance of all security systems.

It is essential that we ensure that systems are deployed effectively, consistently and sustainably:

- Effectively-
  o Systems should be employed in a way that provides us with clear and identifiable benefits.
  o Systems are deployed in proportion to the risks associated to the requirement.
  o System limitations are clearly understood, and elements are correctly specified.
- Consistently-
  o Systems are deployed consistently across UCL.
  o Where possible, the same risk should receive the same specification. Whilst we recognise the need to be responsive to local requirements, specifications should be defined at organisational level, not by local users.
  o Users are given a consistent interface with our systems across different buildings, and can easily understand how they work.
  o Consistency is a key element to comply with data protection requirements, legislation and Government guidance.
- Sustainably-
  o The ongoing maintenance and management of security systems, and the costs associated to this, are an important consideration, and a key driver for the above.
  o The ongoing running costs of maintenance and eventual legacy replacement is an important consideration in the definitions within this specification document.
  o The use of standardized approaches and system components (lock types etc.) ensure that systems can be economically and efficiently maintained and repaired.

UCL has extensive distributed, UCL wide, systems that provide electronic physical security, surveillance and monitoring systems. For the sake of clarity, this document refers to the specification and use of the following systems at UCL:

- Electronic access control/locking.
- Surveillance cameras.
- Alarm monitoring.
- Intercom/door entry systems.

Within the scope of this document is not only buildings owned or wholly leased by UCL, but also where UCL is a tenant in other buildings; in this case the use of the term ‘perimeter’ must be taken to be the perimeter of UCL space within the landlord’s building. Core systems report back to UCL’s central Control Room.
These systems are server based solutions, run on UCL’s data network on secure VLANs managed by UCL’s Information Services Division (ISD).

Due to the growth of UCL, there are some instances where there are local systems that the organisation has inherited with building space acquired through merger etc. These areas may require special consideration, when undertaking works, but the general principle should be that these systems are not extended, but core systems are instead installed, and every opportunity is taken to replace these local systems with our core infrastructure.

2.0 Purpose of document

The purpose of this document is to inform UCL Estates Project Officers and design consultants of the required approach for the deployment of security systems at UCL. This covers both the principles of deployment and technical requirements.

The standards and specifications defined in this document should be taken as part of the Employer’s Requirements of UCL Estates. Where requirements appear to differ from, or not be covered by this document, advice from the UCL Security Systems Manager must be sought.

3.0 Design process, installation and commissioning

It is essential that UCL Security is involved at the earliest stage of the design process in all project work. This should include the design principles for security, detailed system designs and specifications, and the general security processes and procedures for the operation of the building/space.

UCL employs a Specialist Contractor for Security Systems. This contractor maintains and supports all UCL security systems. In addition, this contractor must be employed as part of the project design team, in conjunction with input from UCL Security, to inform the design process of security risks, and create and develop system designs, including detailed specifications and drawings, throughout the project lifecycle, and in line with the RIBA stages (levels of engagement for each stage is detailed in Appendix A). In addition, this contractor must be used to commission all security systems. UCL’s security systems are not building-based stand-alone systems; instead, the functional elements within buildings/areas are simply extensions of the main core, institutional wide systems. No other contractors will be given access to head-end security systems to configure the systems for commissioning new elements.

Appendix A clearly details the involvement and role of our Specialist Contractor for Security Systems as part of Estates project work. As shown, the installation of security systems can be undertaken by another contractor, as long as they subcontract our Specialist Contractor to commission the systems. The main contractor may also choose to instruct our Specialist Contractor to undertake the installation as well as the commissioning element. The installation of all security systems must be undertaken by a competent contractor, and our Specialist Contractor plays a vital role ensuring compliance with the original design and UCL Security’s standards and specifications. Any installation contractor must:
• Adhere to the design and specification provided.
• Comply with any relevant national government or European standards related to electrical or fire safety.
• Install all systems in accordance with the manufacturer’s guidance and standards.
• Be qualified to the following standards (depending on the relevant system):

**General:**
- Contractor must be registered with either SSAIB or NSI.
- Contractor to ISO 14001:2015 Environmental Management System.
- All staff on site to be BS 7858 Security Screened.

**Gallagher system access control and alarm installation:**
- Contractor must be a Gallagher Channel Partner.
- All engineers undertaking wiring on Gallagher components are certified as a minimum to Access Technician (Gallagher Training Level 1/2 C892310).
- Contractor must have one engineer employed, working as part of the installation, trained to System/Access Engineer (Gallagher Training Level 3 C892320).

**Pelco surveillance camera installation:**
- Installation engineers must be Endura 2.0 technician certified.

**Commend intercom installations:**
- All commissioning to be undertaken by Commend themselves or a Commend Certified Premier Partner.
- All commissioning engineers trained to Commend GE300/800 Level 3.

All designs must include complete system drawings and specifications for the project area, and be comprised of:
- Layout drawings showing the deployment of systems with all system elements, including control equipment locations, plotted using agreed iconography.
- Surveillance camera fields of view.
- Requirements for power.
- Requirements for data.
- Requirements for fire alarm system interfaces.
- Containment routes.
- Equipment layouts and drawings showing containment around doors.
- Full specification detailing the following:
  - Detailed operation of system including alarm zoned areas etc.
  - Details of interactions/interfaces with other systems.
  - Types of locking devices required.

### 4.0 Principles of deployment

Referring again to the importance of a consistent approach to the deployment of our systems, below is a reference guide to the instances we would expect to see systems used, how and why.
Notwithstanding this, each project should be designed in conjunction with, and receive sign-off from, UCL Security. The use of our systems outside these principles must be discussed at the earliest stage with the Security Systems Manager.

The environment, and nature of activities at UCL presents many security challenges, so where the requirement falls outside these areas please contact UCL Security for a detailed specification. Contact should be made at the earliest stage to discuss the project requirements and consult the Security Department with regard to the use and design of the systems (see Appendix E - Contact Details). This should be part of the wider discussion that must take place with UCL Security regarding more general security concerns related to all project work. UCL Estates, Security Department reserves the right to make the final decision about how the systems will be deployed, and the specification of installations.

The principles behind the specification of each system deployment is that these systems work together to form consistent and effective security measures, with a clear reasoning behind their deployment, and realistic understanding of their limitations, within the appropriate legislative and good practice guidelines.

4.1 Electronic access control
All comments under this section relate to the use of the Gallagher Security system; the installation of other stand-alone systems is not permitted without the sign-off from the Security Systems Manager, and is likely only in the instances on unavailability of the UCL network.

Electronic card access control should be used for the following applications:

<table>
<thead>
<tr>
<th>Use</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter entrance points.</td>
<td>To secure the entry and exit points of the building providing remote monitoring of door status and audit of activity (not including fire escapes – see alarms section below).</td>
</tr>
<tr>
<td>Turnstiles and MIP entrances.</td>
<td>To provide an anti-tailgating point at main entrances and audit of activity. Card operation of MIP barriers provide easy operation for MIP users.</td>
</tr>
<tr>
<td>Corridors or significant areas within buildings – particularly where this defines departmental boundaries.</td>
<td>To provide security for individual departments, to better enable a secure space within, where free flow of movement can be provided, and the use of less locking points used within the secure space.</td>
</tr>
<tr>
<td>Lifts, where security control is required.</td>
<td>To enable lifts to form part of the secure segregation of space within buildings, or individual lifts to be reserved for specific or hazardous activities.</td>
</tr>
<tr>
<td>Libraries.</td>
<td>To provide an anti-tailgating point at the entrances to Libraries and track entry and exit activity.</td>
</tr>
<tr>
<td>Data Centres.</td>
<td>To provide enhanced security, door status information and alarms, and audit of entry and exit activity.</td>
</tr>
<tr>
<td>Some high security research areas (as defined by UCL on a case by case basis).</td>
<td>To provide enhanced security, door status information and alarms, and audit of entry and exit activity.</td>
</tr>
<tr>
<td>CL3 laboratories.</td>
<td>To provide enhanced security, door status information and alarms, and audit of entry and exit activity.</td>
</tr>
<tr>
<td>Clean rooms where interlocking is required.</td>
<td>To enable both security and environmental interlocks, and ensure electronically locked doors form part of a maintained system to BS 7273-4.</td>
</tr>
</tbody>
</table>
Museums and valuable collections. To provide enhanced security, door status information and alarms, and audit of entry and activity.

Controlled radiation areas. To provide enhanced security, door status information and alarms, and audit of entry and exit activity.

Some patient record storage areas housing NHS Digital data. To provide enhanced security, door status information and alarms, and audit of entry and exit activity.

Main plant rooms, including electrical intake rooms. To ensure the safe and secure management of access to key plant areas.

Roof access. To ensure the safe and secure management of access to roof areas.

### 4.2 Alarm monitoring

Alarm monitoring should include the following applications:

<table>
<thead>
<tr>
<th>Use</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building perimeter doors (typically fire escapes), where these are not controlled by card access control.</td>
<td>To provide a central alarm to alert security that these are no longer secure.</td>
</tr>
<tr>
<td>All new buildings/building refurbishments should include an intruder alarm system protecting the building perimeter.</td>
<td>To enable securing of the space out of working hours or during building closure periods.</td>
</tr>
<tr>
<td>Fire alarm systems activation and fault, to report these signals back to the UCL Control Room.</td>
<td>To report fire alarm activations centrally for action.</td>
</tr>
<tr>
<td>Personal attack/panic alarm point in the following instances:</td>
<td></td>
</tr>
<tr>
<td>1. Main reception points where staff are dealing with members of the public, or specific roles where they may be dealing with confrontational situations.</td>
<td>1. To protect staff who may be subjected to confrontation that may represent a risk to them as part of their role.</td>
</tr>
<tr>
<td>2. Cash handling points (cash tills).</td>
<td>2. As 1 above.</td>
</tr>
<tr>
<td>3. Within unattended student hub space which does not fall under departmental control, where this is available for extended hours.</td>
<td>3. To provide a level of mitigation of risk in instances where the hub spaces are used for extended hours with minimal supervision; and are outside the H&amp;S policies of an individual department.</td>
</tr>
<tr>
<td>4. High security labs or Home Office licence facilities where personal attack represents a risk.</td>
<td>4. As 1 above.</td>
</tr>
<tr>
<td>5. Data centres where personal attack represents a risk.</td>
<td>5. As 1 above.</td>
</tr>
<tr>
<td>MIP and distress alarms, in the following instances:</td>
<td></td>
</tr>
<tr>
<td>1. MIP toilets.</td>
<td>1. To provide conventional distress alert cords/buttons within MIP toilets/facilities.</td>
</tr>
<tr>
<td>2. Dedicated MIP work areas, such as central PC rooms, with minimal or no supervision.</td>
<td>2. To enable an easy method of raising an alert in these areas.</td>
</tr>
<tr>
<td>3. Distress alarms in containment level labs where local and central attention needs to be raised because of an incident or critical spillage.</td>
<td>3. To enable lab users to alert local and central personnel if they have a critical incident within the space that precludes them from leaving the space, and for which they require immediate assistance.</td>
</tr>
</tbody>
</table>

### 4.3 Surveillance cameras

There are several key pieces of legislation to which we are obliged to comply.
In addition to the requirement to comply with the Data Protection Act 1998, the ICO Data Protection Code of Practice for Surveillance Cameras and Personal Information, and the Protection of Freedoms Act 2012; and with the appointment by the UK Government of the Surveillance Camera Commissioner in 2013, organisations are now obliged to work towards compliance with the SCC’s principles and ensure they have consistent strategies for the use of surveillance cameras. To comply with these legislatives and key guidance requirements, it is vital that surveillance cameras are used only in the following instances. This is broken down into areas we would expect to always use surveillance, and areas in which it would be considered on a case by case basis.

UCL Security would expect to see surveillance cameras in these instances:

<table>
<thead>
<tr>
<th>Camera location</th>
<th>What this achieves</th>
<th>Purpose</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>External circulation space.</td>
<td>To enable tracking of suspects/suspicious behaviour.</td>
<td>Observe/Detect.</td>
<td>Yes</td>
</tr>
<tr>
<td>Access points onto main campus.</td>
<td>To achieve facial recognition of persons entering our premises.</td>
<td>Identify.</td>
<td>Yes</td>
</tr>
<tr>
<td>Building perimeter entrance points.</td>
<td>To achieve facial recognition of persons entering our premises.</td>
<td>Identify.</td>
<td>Yes</td>
</tr>
<tr>
<td>Turnstiles at building entrances.</td>
<td>To observe abuse of anti-tailgating turnstiles.</td>
<td>Recognise.</td>
<td>Yes</td>
</tr>
<tr>
<td>Main &amp; public facing reception desks.</td>
<td>To monitor/review any incidents involving members of the public and departmental receptionists’ safety.</td>
<td>Recognise.</td>
<td>Yes</td>
</tr>
<tr>
<td>Library and Museum exits.</td>
<td>View in on final exits viewing any potential thefts via fire escapes.</td>
<td>Identify.</td>
<td>Yes</td>
</tr>
<tr>
<td>High security areas.</td>
<td>Areas such as Radiation Labs, licenced research facilities, CL3, and Data Centres will require some level of CCTV usage (see separate specialist specifications). Typically, this would be aligned with our use of card and PIN on the access controlled point into the space.</td>
<td>Identify/Recognise.</td>
<td>Yes</td>
</tr>
<tr>
<td>Cash handling locations.</td>
<td>To enable monitoring of any cash handling processes taking place on site.</td>
<td>Recognise.</td>
<td>Yes</td>
</tr>
<tr>
<td>Cash machines.</td>
<td>Prevent ‘hold-ups’ or violent confrontations as well as deterring skimming and hidden camera use.</td>
<td>Recognise.</td>
<td>Yes</td>
</tr>
<tr>
<td>Car parks/vehicle entrance points.</td>
<td>To monitor the use of vehicles on campus ensuring safety regulations are adhered to.</td>
<td>Recognise.</td>
<td>Yes</td>
</tr>
<tr>
<td>Bike racks.</td>
<td>To deter and detect any crimes on bikes stored in UCL owned areas.</td>
<td>Recognise/Obsrve.</td>
<td>Yes</td>
</tr>
<tr>
<td>Areas of specific sensitivity or high value.</td>
<td>Areas such as museums, artefacts, internal safes etc., will require some level of surveillance.</td>
<td>Based on requirement.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
UCL Security will consider the use of surveillance cameras in the following instances:

<table>
<thead>
<tr>
<th>Camera location</th>
<th>What this achieves</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
<td>If a department has a specific concern we will discuss options but we may agree a surveillance camera is required for crime prevention or personal safety reasons.</td>
<td>Based on requirement.</td>
</tr>
<tr>
<td>requested cameras following discussions with UCL Security Management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Where lone working security staff are based.</td>
<td>To monitor potential violent confrontations and for the general safety of our staff.</td>
<td>Based on requirement.</td>
</tr>
<tr>
<td>Historical issues/theft hotspots.</td>
<td>If repeated incidents occur in areas not detailed above, surveillance cameras would be considered.</td>
<td>Based on requirement.</td>
</tr>
<tr>
<td>Shop/Café goods.</td>
<td>To deter and detect any shoplifting issues.</td>
<td>Observe.</td>
</tr>
<tr>
<td>Café/Bar seating areas.</td>
<td>To monitor public areas for thefts of phones or bags etc.</td>
<td>Observe.</td>
</tr>
<tr>
<td>Non-departmental student hub/social learning space.</td>
<td>To monitor large student spaces for incidents such as thefts of laptops, phones etc.</td>
<td>Observe.</td>
</tr>
<tr>
<td>Perimeter of buildings.</td>
<td>To deter and detect any criminal damage that may occur to the frontage of our properties.</td>
<td>Observe/Detect/ Monitor.</td>
</tr>
</tbody>
</table>

Alarmed fire escapes are not normally covered by surveillance cameras with the exception of museums and libraries.

Fake surveillance cameras must not be installed; these tend to lead to a false expectation of evidence in the event of an incident.

4.4 Intercom/door entry systems
Where visitors meet a secure point, there may be a requirement to provide a means of communicating with either the building users within, or a central security point, to request access. UCL has three primary deployments:

- IP based network system which uses the main UCL network infrastructure.
- Locally wired intercom/door entry system.
- The use of wall mounted internal telephone extension handsets.

Locally wired solutions should be avoided where possible as these use their own discrete wiring that tends to require regular re-routing to respond to changes in the use of the building. If remote release is required, the IP system is the preferred solution.

Where there is a requirement for the remote release of an access controlled door, a video solution must be provided to ensure that the person who permits entry can identify the visitor to satisfactorily determine that they are authorized to enter.
Typically, these would be specified on the following basis:

<table>
<thead>
<tr>
<th>Use</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main or goods-in building entrances where access is routinely</td>
<td>IP intercom.</td>
</tr>
<tr>
<td>secure with a requirement for remote release.</td>
<td></td>
</tr>
<tr>
<td>Entrances where there is a requirement for remote control by</td>
<td>IP intercom.</td>
</tr>
<tr>
<td>UCL Security.</td>
<td></td>
</tr>
<tr>
<td>Traffic entrances.</td>
<td>IP intercom.</td>
</tr>
<tr>
<td>High security research facilities.</td>
<td>IP intercom.</td>
</tr>
<tr>
<td>Corridor spaces and departmental segregation within buildings.</td>
<td>Internal phone (no remote release).</td>
</tr>
<tr>
<td>Smaller buildings where the requirement is for a large number of</td>
<td>Locally wired (must be agreed by UCL Security).</td>
</tr>
<tr>
<td>handsets throughout the building – making the IP solution</td>
<td></td>
</tr>
<tr>
<td>uneconomic.</td>
<td></td>
</tr>
</tbody>
</table>

### 5.0 Technical specifications

#### 5.1 Access control and alarm monitoring

UCL has a large distributed access control and alarm management system provided by Gallagher Security (see Appendix E – Contact details). This is a server based solution, and runs over a secure VLAN on the UCL network. The Gallagher card access control and alarm monitoring uses a shared infrastructure of networked ‘Controllers’, and downstream local BUS devices (see Appendix B for indicative system architecture schematic).

Operation of the systems is via the UCL ID/smart card for both access control points and alarm arm/disarm terminals. Card and PIN is used in some high security applications.

All electronically locked doors should be managed by this system.

The UCL Security Systems Manager must be consulted with regard to the system architecture design, equipment locations etc., to specify how the new controls will integrate with the existing system, and allow for future expansion. When specifying new infrastructure, Controllers should not be loaded beyond 80% of their maximum capacity of controlling 10 wired, and 20 Aperio doors.

The following specification principles must be observed:

#### 5.1.1 General & equipment

- **5.1.1.1** Gallagher equipment must be installed in Gallagher enclosures.
- **5.1.1.2** All enclosures, including power supply boxes must have tamper signals reporting back through the Gallagher system. URI PSUs can use the integral URI tamper, others will need to assign a separate input. Multiple PSU boxes in one location can have these connected in series. Gallagher Controller and system tamper alarms must not be disabled.
- **5.1.1.3** Contractors must NOT apply their, or any other companies’, logo stickers, other than the manufacturer’s standard label for the equipment, or an asset tag provided by UCL.
- **5.1.1.4** Power supplies units (PSUs) must be provided in plain boxes with no writing other than the manufacturer’s name/model.
5.1.5 Security equipment must be installed directly adjacent to the related fused connection point to facilitate easy isolation.

5.1.6 Fused connection points should be un-switched.

5.1.7 Gallagher controllers must have a dedicated PSU. Readers, locks and local BUS devices should be powered separately.

5.1.8 Where possible, each HBUS URI and related power supply should be installed close to the door it controls. In this instance, the PSU and URI can be located in the same housing.

5.1.9 Battery backup must be provided for all systems. This must provide 4 hours of operation for all control equipment and door locks.

5.1.10 Gallagher Controllers must be installed with DIP switch 1 set to ‘off’.

5.1.11 Network sockets must not be easily accessible, but should be enclosed within a screw lid box – either single gang or 100×100 adaptable box.

5.1.12 All security equipment must be easily accessible for regular servicing, but hidden from view where possible. This can include installations above ceiling level, in cupboards with ‘budget’ locks, behind easily removable panels, at high levels in circulation space where services are generally not covered, etc.

5.1.13 Security equipment must not be installed in plant rooms or riser cupboards.

5.1.14 Steel conduit should be used as standard in preference to PVC, as this offers better mechanical protection and can be easily painted.

5.1.15 Any systems that are decommissioned as part of project works, must be decommissioned back to the power supply, and have all equipment removed. UCL Security must be consulted as to whether this can be reused and should therefore be returned to them.

5.1.16 All systems must be demonstrated as fully working and compliant with the relevant standards, and this document; at the time of, or in advance of, handover of the systems/space to UCL. This must include the release of electronically locked doors by the activation of the fire alarm, to the UCL Fire Officer/Fire Officer’s team.

5.1.17 All access control and alarm installations must be pre-programmed and ready to configure Access Groups and Site Plans at least two weeks in advance of handover of the space to UCL.

5.2 Readers and release mechanisms

5.2.1 Access control readers must be of the T-Series MIFARE type; black with silver bezel.

5.2.2 Readers in exposed areas and vulnerable to physical damage should be installed with a T-Series protective cover.

5.2.3 Where card and PIN, or terminal access is required, T20 readers should be used.

5.2.4 Where T20 readers are used for alarm management only, these should be T20 MIFARE Terminal White.

5.2.5 T20 terminals for alarm management should be mounted between 1200mm and 1400mm from the floor (T20 readers).

5.2.6 Door controls (e.g. door entry systems, readers) should be mounted between 900mm and 1200mm from the floor.

5.2.7 Door readers should be mounted at a consistent height within a single space/building.

5.2.8 All controlled doors without a mechanical means of escape (i.e. lever handle, crash bar etc.) should be released by the fire alarm system, should be of a ‘fail unlocked’ type, and should conform to the UCL Fire Officers Fire Safety Technical
5.1.2.9 All controlled doors without a mechanical means of escape (i.e. lever handle, crash bar etc.) must be installed with a green break glass unit which must be wired to break both positive (+) and negative (-) connections to the fail unlocked lock, and be configured to release on activation of the fire alarm system in accordance with BS EN 7273-4: 2015.

5.1.2.10 Locking mechanisms with a permanently engaged mechanical free exit device, would not normally be configured to release on the activation of the fire alarm.

5.1.2.11 Release of access controlled doors by the fire alarm system should be using the software configuration within the Gallagher system, utilising the primary fire alarm input.

5.1.2.12 Stafford Bridge security doors with the ‘Safe and Secure’ locking solution (see section 5.1.6.6) must have a local fire alarm interface used to cut the power to the fail-locked locking mechanism, along with the local break glass; this then leaves the door secure, but with a free exit handle for easy escape in the event of fire.

5.1.3 Access controlled door monitoring and alarms
5.1.3.1 All access controlled doors must report the following alarm states through the Gallagher system:
   5.1.3.1.1 Unit tamper.
   5.1.3.1.2 Door open too long.
   5.1.3.1.3 Door forced.
   5.1.3.1.4 Door not locked.
   5.1.3.1.5 Fire alarm released door (only required on perimeter doors).
   5.1.3.1.6 Mains failure.
   5.1.3.1.7 Break glass operation.
5.1.3.2 Exit buttons should be of the green button type on a stainless-steel plate marked ‘Press to exit’.

5.1.4 Lift controls
5.1.4.1 Where lifts are controlled by card operation, a reader should be mounted within the lift car to control the operation of the buttons to the required floors.
5.1.4.2 The ground floor button is normally left as free access so that non-cardholders can let themselves out of the building unaided.
5.1.4.3 Each floor must be controlled separately so access can be assigned on a floor by floor basis, or floors left on free access where required.
5.1.4.4 Where all the floors of the lift are controlled, there should also be a reader controlling the use of the lift call button on any publicly accessible floors; to prohibit visitors entering a lift car for which they have no access rights.
5.1.4.5 Integration is achieved through a low-level input/output interface to the lift controls.
5.1.4.6 The Gallagher I/O board should be located as close as possible to the lift controls, but outside the lift motor room.
5.1.4.7 A dedicated junction box with DIN rail connection and clear circuit marking, must be installed to mark the clear separation between the two systems to ensure that engineers can easily isolate systems for diagnosing faults.

5.1.5 Other system integrations/interfaces
5.1.5.1 Where access control is integrated with automated door operators (but where the lock is controlled directly by the Gallagher system) the system must be installed with MIP buttons on both entrance and exit to ensure that the system will function fully in free access mode.

5.1.5.2 This is achieved by the use of a four pole/two way relay and a timer relay. See Appendix D.

5.1.5.3 In all instances, it is preferable that the lock is controlled directly by the Gallagher system, and that the only exceptions for this should be when the nature of the automated door system provides no option but to provide a simple trigger to operate.

5.1.5.4 For integration with turnstiles, and the specification of the turnstiles themselves, please refer to the separate UCL specification document – available by request from the Security Systems Manager.

5.1.5.5 Where fire alarm activated door hold-open devices are installed on doors which require access control, these must be integrated with the access control system. This is done by wiring the power to the hold-open device through a relay provided as part of the access control installation. This relay is activated by the lock relay status (for single doors) or the door open too long signal (for double doors); and this then must cut the power to the hold-open device when the Gallagher system sets the door to secure access. This is to ensure that when doors change from free access periods to locked periods, the operation of the hold-open device does not conflict with the electronic locking and require manual intervention. The relay should be in a separate adaptable box as a clear point of separation between the two systems.

5.1.6 Locking and security doors

5.1.6.1 It is essential that the choice of locking mechanism is in proportion to the requirements. This table shows the main options – Full list of approved locks is available in Appendix C. Only the listed lock types may be specified – Any requirement to vary from this must be agreed by the Security Systems Manager:

<table>
<thead>
<tr>
<th>Type</th>
<th>Security level</th>
<th>Use</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maglock 250.</td>
<td>Low</td>
<td>General corridor areas, single or double doors.</td>
<td>Low maintenance, but low security and fails unlocked.</td>
</tr>
<tr>
<td>Maglock 500.</td>
<td>Low/Moderate</td>
<td>Building entrances and high use areas.</td>
<td>Low maintenance, and fails unlocked.</td>
</tr>
<tr>
<td>Abloy EL560.</td>
<td>Moderate/High.</td>
<td>Medium/high security areas.</td>
<td>Can only be used on single doors. Cannot be used with controlled exit. Fails locked with key override.</td>
</tr>
<tr>
<td>Abloy EL561.</td>
<td>Moderate.</td>
<td>Medium security areas.</td>
<td>Can only be used on single doors. Can be used for controlled exit. Fails unlocked with key override.</td>
</tr>
<tr>
<td>Abloy EL520.</td>
<td>Moderate/High.</td>
<td>Medium/high security areas.</td>
<td>Similar to EL560, but motorised to use with automated operators.</td>
</tr>
<tr>
<td>ASSA 5331A electric strike.</td>
<td>Moderate.</td>
<td>On entrances where maglocks are not practical.</td>
<td>Useful for historic doors for discreet installation. Only suitable for single doors.</td>
</tr>
</tbody>
</table>
5.1.6.2 All double and leaf-and-a-half door sets must have both leaves locked by the system.

5.1.6.3 All access controlled doors must be installed with an effective closing mechanism of the appropriate type on both leaves.

5.1.6.4 All rebated or lipped double or leaf-and-a-half door sets, must be installed with an effective selecting mechanism, so that the door leaves shut in the correct order and the doors lock effectively without manual intervention.

5.1.6.5 Where access control points represent the perimeter of UCL space (these would be either street level entrances into our buildings, or entrances into UCL space from within third-party landlord’s buildings), where the locking is of the fail-locked type - in addition to the access control locks, a mechanical europrofile deadlock must be installed to provide the ability to secure the building in the event of extended system or power failure.

5.1.6.6 Where there is a requirement for LPS rated security doors, these must be provided by Stafford Bridge (http://www.staffordbridge.com/). The table below provides guidance for their application:

<table>
<thead>
<tr>
<th>Door type</th>
<th>Security level</th>
<th>Lock type</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abloy 351U80</td>
<td>Moderate</td>
<td>Medium security areas</td>
<td>Can be used on double doors, but must be well fitting.</td>
</tr>
<tr>
<td>Abloy 351M80</td>
<td>Moderate</td>
<td>Medium security areas</td>
<td>Motorised version of the above, for use on doors which are free access for periods.</td>
</tr>
<tr>
<td>Abloy Aperio L100</td>
<td>Moderate</td>
<td>Student accommodation rooms</td>
<td>This is for card operation of student bedrooms, and provides EN170 compliant escape.</td>
</tr>
<tr>
<td>Stafford Bridge - Surelock McGill</td>
<td>High/Critical</td>
<td>High security research areas – Available in SR3 and SR4 variants.</td>
<td>Available in controlled and free exit variants.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Door type</th>
<th>Security level</th>
<th>Lock type</th>
<th>Application</th>
</tr>
</thead>
</table>
| Sandhurst. SR3.            |                | Controlled entry / Free exit SL325 (SL325-00-K2MNO2PW). | • Licenced research facilities.  
                                |                |                                               | • CL3 labs.  
                                |                |                                               | • Controlled radiation areas. |
| Sandhurst. SR3.            |                | Controlled entry & exit Safe and Secure (S-11250-0X-MNO2P). | • Licenced research facilities.  
                                |                |                                               | • CL3 labs.  
                                |                |                                               | • Controlled radiation areas.  
                                |                |                                               | • Where interlocking is required. |
| Wilton or Halton. SR4.     |                | Controlled entry / Free exit SL325 (SL325-00-K2MNO2PW). | Data centres with no interlocking requirement.                              |
| Wilton or Halton. SR4.     |                | Controlled entry & exit Safe and Secure (S-11250-0X-MNO2P). | Data centres where interlocking is required.                                |
5.1.6.7 It should be noted that to retain the LPS rating while the space is in use, the installation will require an interlocking pair of doors with both doors complying to the required standard, to ensure that the LPS rated enclosure retains its’ integrity when one of the doors is open.

5.1.6.8 Consideration will need to be given to the construction of the space itself – including walling, plant louvres and windows.

5.1.7 **Alarm monitoring**

5.1.7.1 All alarm inputs must be installed with the correct end of line (EOL) resistors to provide four state monitoring (open/closed/open circuit tamper/closed circuit tamper). This must be a series and parallel pair of 4K7 resistors. These must always be installed at the end of line to ensure tamper protection of the whole circuit.

5.1.7.2 Where an arming point is required, this should be in the form of a T20 in white finish mounted between 1200mm and 1400mm from the floor.

5.1.7.3 Fire alarm signals must be brought back to UCL's central Control Room via the Gallagher system. This must include activation and fault. The fire alarm system interface module must be installed immediately adjacent to a Gallagher Controller, to minimise the reliance on non-fire rated cable. EOL resistors must be mounted inside the fire alarm interface module.

5.1.7.4 The Gallagher system must be setup to create an alarm related to all fire alarm activation inputs when any dependant signal path devices stop communicating with the server, to alert security to the loss of these fire signals.

5.1.7.5 MIP toilet and other distress alarms must be Timeguard Emergency Assist Alarm units ([http://www.timeguard.com/products/safety/emergency-assist-alarms](http://www.timeguard.com/products/safety/emergency-assist-alarms)). These should be specified with a local panel to alert passers-by, or lab managers or other responsible persons. They must also be connected to an input on the Gallagher system, interfaced with a separate relay.

5.1.7.6 At fixed staffed points (receptions/cash handling etc.), panic/personal attack alarms should be located in a discreet, easy to access location, where the operator can trigger the device unobserved. Where these are used in facilities, rather than at fixed locations, these should be located around the facility – this must include immediately adjacent to the entrance of the facility (inside), and at a convenient run-back point in case the user opens the door to a threatening situation.

5.1.8 **Intruder alarms systems**

5.1.8.1 Intruder alarm system door contacts must be separate from those used for access control, so where access controlled doors also represent a perimeter zone on the intruder alarm system, this would have two separate sets of door contacts.

5.1.8.2 Full perimeter protection must be provided covering all accessible windows and doors using door contacts and dual-tech motion sensing. This must include any accessible points above ground level where there could be intrusion via another building (e.g. accessible roofs etc.).

5.1.8.3 Where door contacts are used, motion sensing should be used to confirm intrusion inside the space.

5.1.8.4 The use of motion sensing should be specified so that this does not rely on single devices, but provides a level of confirmation from secondary devices.

5.1.8.5 Acoustic glass break sensors should be used in all areas where there are accessible windows. These should be programmed on a 24 hour circuit.
5.2 Surveillance cameras

UCL has a site wide Pelco Endura security surveillance camera and video management system. This runs on a secure VLAN on the UCL network. This comprises of management storage devices, cameras, workstations and decoders.

5.2.1 All cameras must be from the Pelco Enhance+ (IME+/IXE+Next Gen) range.
5.2.2 All dome cameras (including internal) must be of the Environmental Housing (Env) type, with a clear dome.
5.2.3 Fixed external cameras would normally be the IXE+ Sarix Enhanced box camera range, in IP66 POE housing.
5.2.4 Cameras should be mounted on a wall or fixed ceiling wherever possible. Cameras should not be installed into removable ceiling tiles/elements.
5.2.5 The network socket should be installed immediately adjacent to the camera, inside an enclosure to avoid tamper issues; this can be done either within a single gang blank box, or by mounting the network socket within a 100×100 adaptable box. Exceptions to this must be signed off by the UCL Security Systems Manager.
5.2.6 See the table below, and read in conjunction with section 4.3 Surveillance cameras (design), that lists the applications and requirements for surveillance cameras. It is essential that all surveillance camera images are effective for the purpose for which the camera has been installed, and that they have a clear purpose. We use this to define the standards, accepted requirements, and limitations of use, for surveillance cameras at UCL. As the Rotakin evaluation in terms of percentage of the image is essentially redundant with higher resolution IP cameras, this is included for reference only. The appropriate camera must be installed in each instance, to achieve the minimum pixels per metre (PPM) for each camera purpose category: Please refer to this in conjunction with section 4.3 Surveillance cameras.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Rotakin value</th>
<th>PPM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inspect</td>
<td>250%-300%</td>
<td>1000 pixels/m</td>
</tr>
<tr>
<td>Identify</td>
<td>100% - 120%</td>
<td>250 pixels/m</td>
</tr>
<tr>
<td>Recognise</td>
<td>50%</td>
<td>125 pixels/m</td>
</tr>
<tr>
<td>Observe</td>
<td>25%</td>
<td>62.5 pixels/m</td>
</tr>
<tr>
<td>Detect</td>
<td>10%</td>
<td>25 pixels/m</td>
</tr>
<tr>
<td>Monitor</td>
<td></td>
<td>12.5 pixels/m</td>
</tr>
</tbody>
</table>

5.2.7 Camera height will be by and large application dependant, but cameras used to identify, should be installed at a height of 2.4m where possible.
5.2.8 When installing cameras at heights above 3m – This should be avoided whenever possible, but if operationally required, consideration must be given to the way this changes the efficacy of the camera and views that it achieves. In addition, careful consideration must be given to the serviceability of the camera bearing in mind working at height issues related to servicing.
5.2.9 Consideration must be given to the use of cameras used in reduced lighting conditions, where IR lighting may be required to provide effective images – either internally or using external lamping.
5.2.10 Commissioning documentation must demonstrate the performance of cameras in both day and night lighting conditions.
5.2.11 For works that include more than 5 cameras, project teams must discuss with the UCL Security Systems Manager the impact on data storage that the addition of new
cameras will have on the system infrastructure. A charge may be levied to compensate for the cost impact for the additional data storage requirement.

5.2.12 Where project work changes the use of the space, and therefore requires the reassessment of surveillance camera purposes and effectiveness; this must form part of the security review within the project. The Home Office’s Surveillance Code of Practice requires the regular review of the effectiveness and purpose of cameras, and this is particularly essential where a change of the use of the space potentially changes the original purpose of the cameras.

5.2.13 Cameras should be POE powered from the UCL network switch without the use of injectors or separate power supplies; except where IR lamping requires this.

5.2.14 UCL does not currently have an integration of Pelco software with our institutional desktop PC build. All hardware must be specified as Pelco proprietary devices, including workstations and decoders, with the exception of

5.2.15 For decoder installations requiring only 4 viewing images, the BBV Asgard HD Decoder and mounting bracket (OV-HD01 & OV-HA01) should be used.

5.3 Intercom/door entry systems

UCL has two approved solutions for intercom systems – Commend and BPT. The Commend system is our preferred solution. The Commend system is an IP based video intercom solution, that enables us to deploy this across the site with centralised control. The BPT solution is a locally wired alternative that should only be used when the Commend solution is impracticable because of the cost of deployment. The use of the BPT system as an alternative to the preferred solution must be signed off by the UCL Security Systems Manager. The main advantages of the Commend system is the very high standard of audio and video quality and the flexibility of relocating handsets as they use the UCL network infrastructure. The main disadvantage of the BPT solution is the local wiring that becomes expensive to modify as the requirement for handset positions tends to change over time.

5.3.1 Where internal corridors are locked, we would not normally install intercom systems, but would expect to see a wall mounted internal telephone extension with a list of numbers to call.

5.3.2 Where an intercom is required to have remote release of an access controlled door, this must provide both audio and video to the user to ensure they are able to differentiate valid requests from visitors.

5.3.3 The physical release output from the intercom must never be taken from an output on the exterior call point, but only from the ‘safe side’ equipment. With the Commend system, these input/output interfaces with Gallagher are all physically wired directly into the Gallagher system using Gallagher I/O devices adjacent to the Commend server devices.

5.3.4 The Commend system uses a central solid state ‘server’ device; this is updated with physical expander cards and licences to enable expansion. The provision of cards and licences must be included as part of all installations.

5.3.5 The system is divided into Master (the handset responder unit) and Slave (intercom panel at the door) stations. As a preference, and where possible, master units should be wall mounted to minimise the risk of these being removed by users.

5.3.6 When installed in lab/clean room environments, the wipe-down foil surface units should be used.

5.3.7 The Commend system is essentially a video VOIP solution. At installation, this should be configured as separate ‘systems’ whereby the users are not able to ‘call out’ to
other devices – this is an essential privacy feature (the security central master stations being the only exception to this):

5.3.7.1 Commend system must be installed so that local users cannot see other subscribers, outside their group, in the ‘Show video’ menu function.  
5.3.7.2 Commend systems must be installed with the ‘Show live video’ function off.  
5.3.7.3 Commend systems must be installed with the ‘Privacy’ function on as default.

5.3.8 Where BPT systems are used, these must be of the X1 or XIP system; using only physical wired solutions.

5.3.9 All BPT devices should be wired with CAT 5e and 1mm² pair for power between all devices.
Appendix A – Security Systems Specialist Contractor

This schematic shows the relationships of UCL’s Security Systems Specialist Contractor to UCL’s design teams and main contract teams.

There are two separate and distinct relationships:

1. Employed as part of UCL’s design team.
2. Employed by the main construction contract (or sub-contractor) as the commissioning contractor.

As described, additionally the construction contractor may also choose to employ UCL’s Security Systems Specialist Contractor as the systems installer, but is not obliged to do so.

---

**UCL Design team**

Architects | PM | M&E | QS | Security Specialist Contractor

---

**Security Specialist Contractor working with UCL’s design team & UCL Security throughout RIBA stages**

---

**RIBA Stage 1**
Preparation & Brief

- Early engagement to assess if there are particular security concerns that should inform the design approach.
- Alert the design team to any particular key requirements related to the building designs on which the future security designs might rely.

---

**RIBA Stage 2**
Concept Design

- Undertake a more detailed risk analysis.
- Develop security system design concepts to a point where principle controlled zones are established, and there is an understanding of the types of controls applied to each zone.
- Further development of some more detailed key principles in projects where there is a higher security risk.
- Highlight areas of the design where security risks should inform design specifications or related elements, e.g. door types, wall construction etc.
- Develop initial projected costs.

---

**RIBA Stage 3**
Developed Design

- Work with design team and client to clarify all detailed requirements.
- Completion of detailed designs including:
  - Produce specification of all system types.
  - Creation of a detailed functional specification which describes the operation of the systems.
  - Details of any integrations or interactions with other systems.
- Completion of drawings showing all system components, and containment requirements.
- Provide detailed projected costs.

---

**RIBA Stage 4**
Technical Design

- Work with construction contractor during construction phase to ensure compliance with agreed specification.
- Respond to requirements for changes and alterations during construction.
- Update drawings and designs as required during this phase.

---

**RIBA Stage 5**
Construction

- Completion and issuing of ‘as constructed’ security system drawings and system specification.

---

**RIBA Stage 6**
Handover & Close Out

- System commissioning - instructed by contract.

---

**Main Contractor**

Electrical Sub-contractor

---

Separate to being employed working with UCL’s design team, UCL’s Security Specialist Contractor must also be instructed by the Main Contractor (or his electrical subcontractor) to commission relevant systems (at tendered commissioning rates). In addition, the main contract may choose to use our Specialist Security Contractor to install system, but they are not obliged to do so.
Appendix B – Gallagher system architecture schematic

This schematic shows the relationship between the Gallagher server, Controllers and downstream BUS devices.
Appendix C – Approved lock types

Only the following lock types may be specified – Any requirement to vary from this must be agreed by the Security Systems Manager:

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Model</th>
<th>Accessories</th>
<th>Type</th>
<th>Security level</th>
<th>Use</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adams Rite</td>
<td>261-005 (Single) 262-005 (Single)</td>
<td>Z&amp;L brackets, architectural cover plates</td>
<td>Maglock 250</td>
<td>Low</td>
<td>General corridor areas, single doors</td>
<td>Low maintenance but low security and fails unlocked (250Kg holding force)</td>
</tr>
<tr>
<td>Adams Rite</td>
<td>261-205 (Double)</td>
<td>Z&amp;L brackets, architectural cover plates</td>
<td>Maglock 250</td>
<td>Low</td>
<td>General corridor areas, double and leaf-and-a-half doors</td>
<td>Low maintenance, but low security and fails unlocked (250Kg holding force)</td>
</tr>
<tr>
<td>Adams Rite</td>
<td>281-005 (Single) 291 (External single)</td>
<td>Z&amp;L brackets, architectural cover plates</td>
<td>Maglock 500</td>
<td>Low/Moderate</td>
<td>Building entrances and high use areas, single door</td>
<td>Low maintenance, and fails unlocked (500Kg holding force)</td>
</tr>
<tr>
<td>Abloy</td>
<td>EL560/65</td>
<td>Must be installed with approved handles (Futura) to achieve EN179, EA288/02 split spindles and EA280 door loop. 65mm, backset should be used as standard, but others available when restrictions apply</td>
<td>Abloy EL560 Solanoid lock</td>
<td>Moderate/High</td>
<td>Medium/high security areas</td>
<td>Can only be used on single doors. Cannot be used with controlled exit. Fails locked with key override</td>
</tr>
<tr>
<td>Abloy</td>
<td>EL561/65</td>
<td>As above</td>
<td>Abloy EL561 Solanoid lock</td>
<td>Moderate</td>
<td>Medium security areas.</td>
<td>Can only be used on single doors. Can be used with controlled exit. Fails unlocked with key override</td>
</tr>
<tr>
<td>Abloy</td>
<td>EL520/65</td>
<td>As above</td>
<td>Abloy EL520 Motorised lock</td>
<td>Moderate/High</td>
<td>Medium/high security areas</td>
<td>Similar to EL560, but motorised to use with automated operators</td>
</tr>
<tr>
<td>Manufacture</td>
<td>Model/Description</td>
<td>Suitability</td>
<td>Application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASSA</td>
<td>S331A</td>
<td>Moderate</td>
<td>On entrances where maglocks are not practical. Useful for historic doors for discreet installation. Only suitable for single doors. Opens under side load.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abloy</td>
<td>Aperio L100 escutcheon (BL560)</td>
<td>Moderate</td>
<td>Student accommodation rooms. This is for card operation of student bedrooms, and provides EN170 compliant escape.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abloy</td>
<td>351U80 Optional strike plates</td>
<td>Moderate</td>
<td>Medium security areas. Can be used on double doors, but must be well fitting.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Abloy</td>
<td>351M80 Optional strike plates</td>
<td>Moderate</td>
<td>Medium security areas. Motorised version of the above, for use on doors which are free access for periods.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surelock McGill*</td>
<td>Slimline Multipoint - SL325 (SL325-00-K2MNO2PW)</td>
<td>Free exit variant. Must have locking and request-to-exit monitoring.</td>
<td>These are the locking systems integral to the Stafford Bridge LPS rates security doors. Free exit variant.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Surelock McGill*</td>
<td>Slimline Multipoint – Safe and Secure (S-11250-0X-MNO2P)</td>
<td>Secure/controlled exit variant. Must have locking and request-to-exit monitoring</td>
<td>These are the locking systems integral to the Stafford Bridge LPS rates security doors. Secure exit variant.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix D – Miscellaneous specification details
Reference 5.1.5.2 – Integration of automated door operators

All relays shown when the door is in secure mode
Appendix E – Contact details

UCL Security Systems Manager:
   Mike Dawe  
   m.dawe@ucl.ac.uk  
   020 7679 7735

Security System Specialist Contractor:
   Reliance High-Tech Ltd  
   100 Berkshire Place  
   Wharfedale Road  
   Winnersh  
   Wokingham  
   Berkshire  
   RG41 5RD  
   Tel: 0845 121 0802  
   https://www.rht.co.uk/  
   Contact for UCL works: Keith Dixon keith.dixon@rht.co.uk

Gallagher Security (Europe) Limited  
   Security House  
   Unit 5 Eastboro Fields  
   Hemdale Business Park  
   Attleborough  
   Nuneaton  
   Warwickshire  
   CV11 6GL  
   Tel: 024 7664 1234  
   Email: info.eu@security.gallagher.com  
   https://security.gallagher.com/

Pelco by Schneider Electric  
   Indigo House  
   Mulberry Business Park  
   Fishponds Road  
   Wokingham  
   United Kingdom  
   RG41 2GY  
   01189 789 276  
   https://www.pelco.com/

Timeguard Emergency Assist Alarms  
   Timeguard Limited Victory Par  
   400 Edgware Road  
   London  
   NW2 6ND  
   http://www.timeguard.com/