Security Needs Assessment
UCS School, London

Figure 01 - Proposed Sketch (Source: Ed Toovey Architects)

Document Number:	R121-KS-SY-ZZ-RP-Y-0001-S4-A	
Revision:	A	
Date of Issue:	01/11/2023	
Status:	Issued for Review	
Author:	NH	
Distribution:	Edward Toovey	Ed Toovey Architects

Kabsec Consultancy Ltd
Security Risk Management

1 Executive Summary

This report describes a Security Needs Assessment (SNA) completed by KABSEC in support of the design and construction of the changes to University College School, Hampstead, London, NW3 6XH.

The SNA considers security threats to the proposed development and security vulnerabilities apparent in the architectural designs and proposed uses. The SNA follows a security design methodology to provide security recommendations that should be designed and specified in future project stages. These recommendations are specifically intended to mitigate security risks to the development, its users, and the surrounding area.

1.1 BREEAM Hea 06 Security credits

The activities are undertaken and the structure and content of this report are aligned with the requirements of BREEAM RFO 2014 Hea 06.

1.2 Security Recommendations

This SNA report provides a suite of security risk mitigation options for consideration. These recommendations aim to mitigate the security risks to the development in a pragmatic and proportionate manner while considering their potential impact on the proposed budget, operation, and appearance of the building.

Comments on the security recommendations in this report are invited from the client and design team, in order to ensure compatibility with operation, design, and budget.

2 BREEAM RFO 2014 Hea 06 Security - Requirements

"A Suitably Qualified Security Specialist (SQSS) conducts an evidence-based Security Needs Assessment (SNA) during or prior to Concept Design (RIBA Stage 2 or equivalent)"

KABSEC staff are licensed under both the Secured by Design (SBD) and Security Assurance BRE (SABRE) security accreditation schemes.

The SNA requirements were completed in Oct and Nov 2023, during RIBA Stages 2.

"The SQSS develops a set of recommendations or solutions during or prior to Concept Design (RIBA Stage 2 or equivalent). These recommendations or solutions aim to ensure that the design of buildings, public and private car parks and public or amenity space are planned, designed and specified to address the issues identified in the preceding SNA"

Security recommendations are described in this report, covering each area listed above where relevant.

"A visual audit of the site and surroundings, identifying environmental cues and features pertinent to the security of the proposed development"

BREEAM permits the completion of the visual audit via a "review of relevant project information and drawings, provided the SQSS is satisfied that these are sufficient to inform their SNA & associated security recommendations".

A visual audit was therefore completed using Google Maps, and open-source crime data including crime statistics from police.uk.

"Formal consultation with relevant stakeholders, including the local ALO, CPDA & CTSA (as applicable), in order to obtain a summary of crime and disorder issues in the immediate vicinity of the proposed development"

A meeting with the Metropolitan Police Service Designing Out Crime Officer was requested. We have received a response stating: *'Please note we do not provide a consultation service solely for the purposes of meeting the BREEAM Security Needs Assessment (SNA) to achieve a credit under heading HEA06'.*

"Identify risks specific to the proposed, likely or potential use of the building(s)"
"Identify risks specific to the proposed, likely or potential user groups of the building(s)"

- Described in the relevant section of this report.

"Identify any detrimental effects the development may have on the existing community"

- KABSEC cannot identify any detrimental effects to the existing community.

"The recommendations or solutions proposed by the SQSS are implemented"

- To be confirmed by the BREEAM Assessor on completion of the project.

3 Development & Surroundings

3.1 Visual Audit

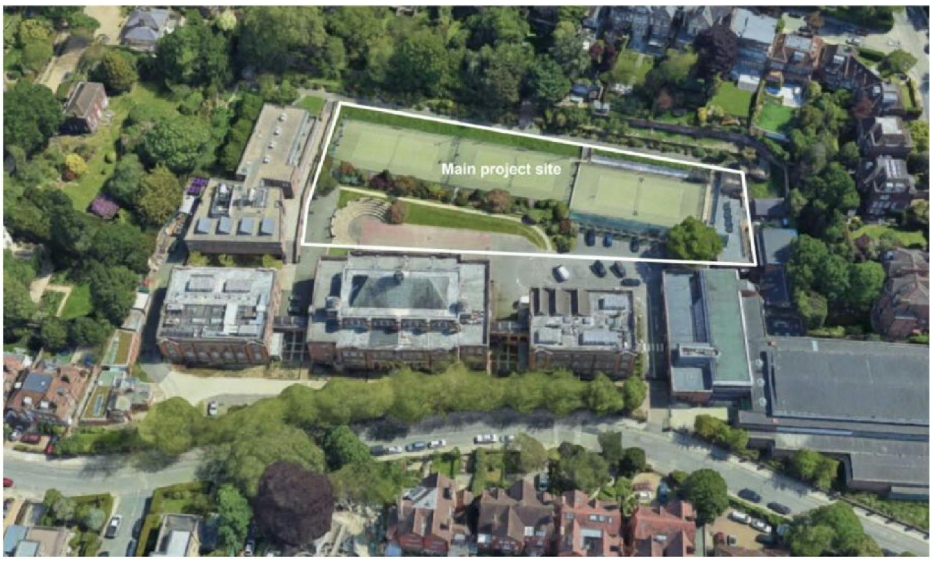


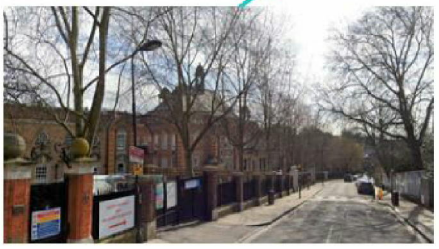
Figure 02 - Location Plan (Source: Ed Toovey Architects)

University College School (UCS) is a prestigious independent school located in Hampstead, London, NW3 6XH. The school is surrounded by the vibrant Hampstead Village, the expansive Hampstead Heath, cultural attractions, and other renowned educational institutions like University College London (UCL).

Its location offers students access to a diverse range of experiences and resources, and it is well-connected to the rest of London via the London Underground's Northern Line, providing convenient transportation options for students, staff, and parents. This makes it an ideal place for academic and personal growth.

The main part of the proposals will be a single-storey building at ground level, with three tennis courts on the roof, replacing existing courts. At the south end of the site, the building rises to 2-storey above ground and contains the more specialised facilities, including a dedicated new Music Recital Room, a Cafeteria, and Drama Studios. As the rear of the site is terraced on sloping ground, a substantial new retaining wall will be required for the building, supplementing an existing retaining wall which is to be partially re-used.

4 Site Survey



5 Development Layout & Uses

5.1 Ground Floor Plan

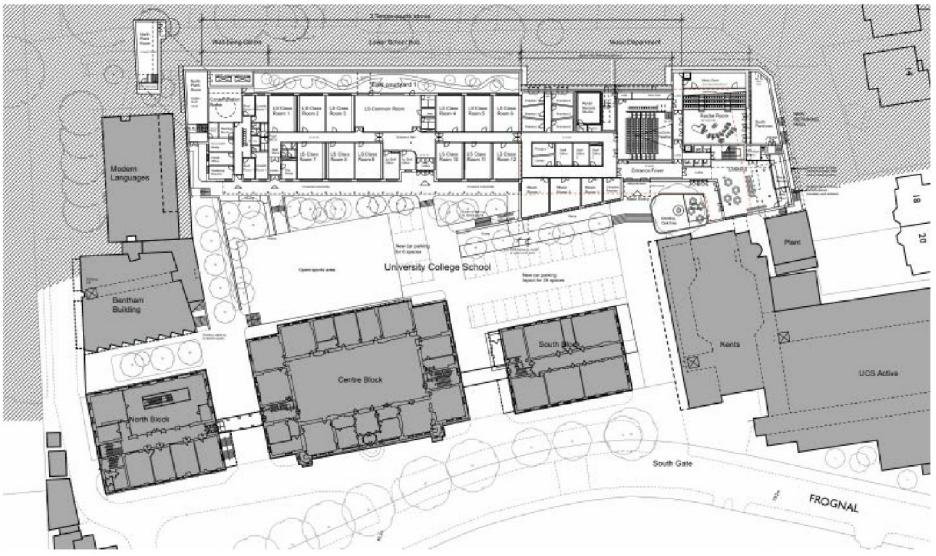


Figure 03 - Ground Floor Plan (Source: Ed Toovey Architects)

The ground floor will consist of an Entrance Foyer, Cafe, Recital Room, lecture Theatre, Music Rooms, Rock/Record Studio, Classrooms, Comms Rooms, Meeting Rooms, Plant Rooms, Contemplation Room, Counsellors Study, PSHE Office, Well-being Directors Office, Consultation Room, Rest Room, Staff Offices, Practice Room, Library, General Store Rooms, Courtyard, WCs, Core Stairs and Lifts.

5.2 First Floor Plan

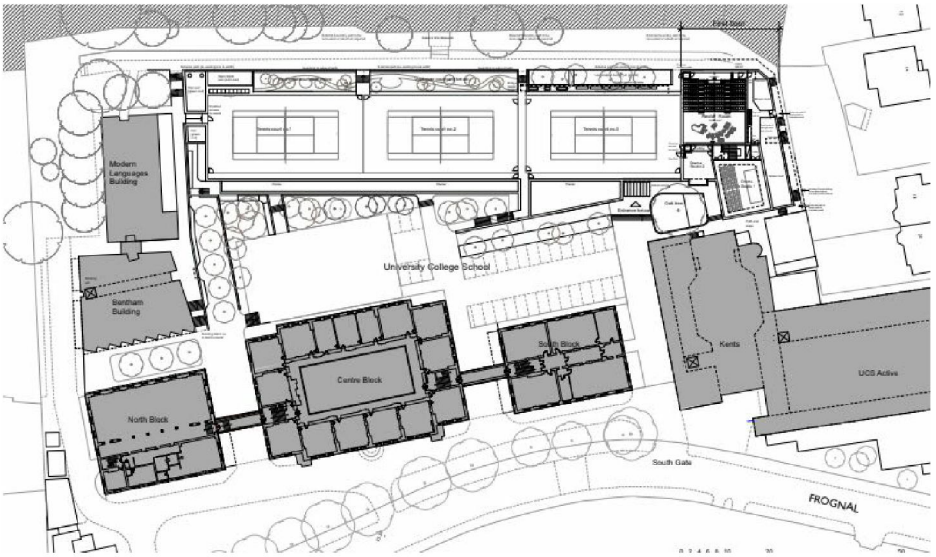


Figure 04 - First Floor Plan (Source: Ed Toovey Architects)

The first floor will consist of a Recital Room, Drama Studios, Tennis Courts, Green Roof, Brown Roofs, Plant Spaces, WCs, Core Stairs and Lifts.

6 Crime Risk Assessment

KABSEC uses police crime statistics to support our assessments of crime risks. Police statistics consider the development site to be within the Frognal 'policing neighbourhood' within the Metropolitan Police Service force area.

6.1 Frognal

https://www.police.uk/pu/your-area/metropolitan-police-service/frognal

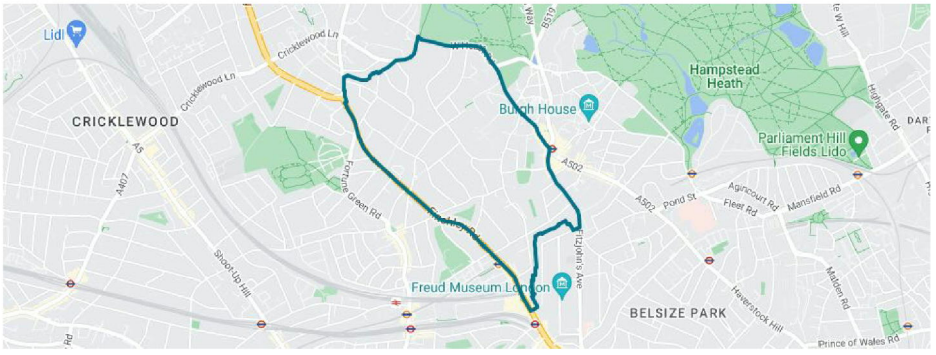


Figure 05 - Frognal 'Policing Neighbourhood'

Information accessible on www.police.uk reveals that crime and disorder in that area within the preceding 12 months were dominated by:

- Vehicle Crime
- Anti-social Behaviour
- Violence and Sexual Offences
- Burglary

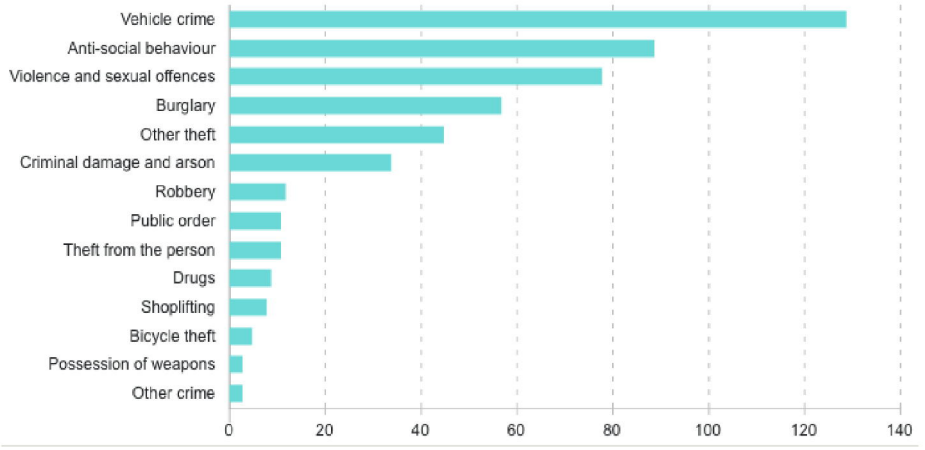


Figure 06 - All crime types in Frogal between Sep 2022 to Aug 2023.

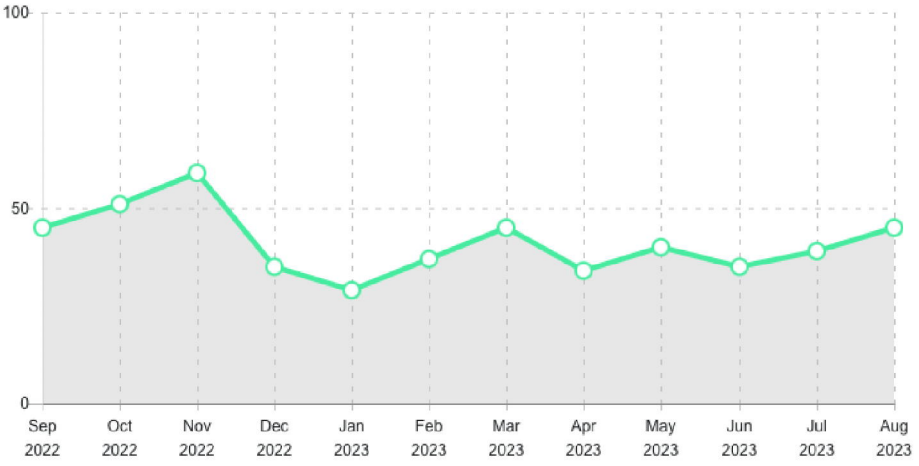


Figure 07 - All crime levels in Frogal between Sep 2022 to Aug 2023.

The crime rate peaked in Nov 2022 dominated by vehicle crime and violence and sexual offences. The lowest recorded crime recorded was in Jan 2023 dominated by burglary and vehicle crime.

Threat Actors	Description	Reasonable Worst-Case Scenario
Threat - Opportunist Theft	Opportunist theft affects educational properties where a criminal in a legitimate location (e.g. reception area or car park) can readily observe a security vulnerability. Anecdotally, including police crime reporting, most opportunistic theft involving intrusion occurs through doors that have been left open, unlocked or unattended. The capability of opportunist thieves is also typically considered to be low, as they are unwilling to carry tools that could be considered as 'going equipped'.	A single threat actor attempts to breach the building envelope through open or unlocked doors or windows. Novice attackers with no tools. Covert.
Threat - Deception Theft	Similarly to opportunist theft, the use of deception to enter a premises is often seen as a lower risk on the part of the criminal. Commonly reported examples include criminals posing as services engineers or the authorities to convince building management staff to allow them access to a property, or a wide range of deceptions in order to effect the opening of a door to enable a violent entry.	A single threat actor attempts to breach the building by posing as a service engineer or the authorities to convince building management staff to allow them access to a property Not categorised as overt or covert.
Threat - Targeted Theft	Educational properties can be targeted by professional organised criminals for intrusion and theft if they are perceived to contain high-value portable items such as school equipment and electronic devices.	Multiple threat actors attempt to breach the building envelope and internal security features using a range of hand tools. Overt. Experienced and knowledgeable attackers, using concealable hand tools and electronic devices. Covert.

6.2 Security Threat Categories

The table below categorises the previously discussed threats based on capability and intent, i.e. the number of attackers, their level of expertise and fitness, willingness to be caught or harmed and the tools and weapons available to them.

The table below combines similar threat actors into the same attack category, to provide a summary of potential 'reasonable worst-case' threats.

Attack Category	Reasonable Worst-Case Threat
Opportunistic Theft	A single threat actor attempts to breach the building envelope through open or unlocked doors or windows. Novice attackers with no tools. Covert.
Vandalism	A single or multiple actors deliberately destroying of or damage to public or private property. Novice attackers with improvised tools. Overt.
Anti-social Behaviour	Multiple actors causing harassment, alarm, or distress to a community, public spaces, or buildings. Novice attackers with no tools. Overt.
Targeted Theft	Multiple threat actors attempt to breach the building envelope and internal security features using a range of hand tools. Overt. Experienced and knowledgeable attackers, using concealable hand tools and electronic devices. Covert.
Mob Attack	Multiple threat actors attempt to damage the building and to breach the building envelope. Novice attackers with improvised tools. Overt.

6.3 Layering Security Measures

The effectiveness of security risk mitigation measures in combination is typically considered using a layered, or onion skin model comprising:

- Electronic security measures including intruder detection, video surveillance, and access control to provide to alert responders to threats

- Physical security measures including fences, vehicle barriers, walls, doors, and safes to deny or delay threat actors reaching their targets

- Operational security measures including procedures, risk assessment, monitoring, patrolling, and response.

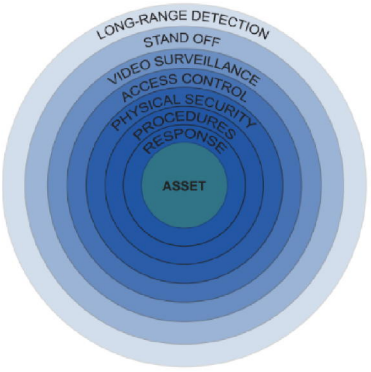


Figure 08 - 'Onion Ring' Model

In an urban setting, these layers are typically represented by:

- External Intrusion Detection Systems
- Boundary treatments and landscaping
- Video Surveillance
- Doors and Windows
- Internal Intruder Detection Systems
- Hold-up Alarm Systems (panic buttons)
- Refuge Areas
- Security guards, third-party security or police response

7 Security Design Requirements

7.1 Design Basis Threats

Based on the threat categories highlighted earlier, the following table focuses on the 'reasonable worst-case' attack types that are proposed for specifying security measures.

These are used as the 'design basis threats' (DBTs) for the specification of security measures.

7.2 Eductional Property DBT's

Attack Category	Description
Novice attackers with no tools.	A single threat actor attempts to breach the building envelope through open or unlocked doors or windows.
Experienced forced entry using manual attack.	Two experienced aggressors using concealable hand tools to attempt entry into the building. The attack may generate some noise but will be intended as surreptitious.

8 Security Requirements Statements

The Security Requirements Statement:

1. Categorises the various influencing factors into clear statements that can be addressed through security design and operating procedures

2. Ensures that security needs and project constraints are understood before security solutions are considered

3. Forms the basis for the specification of security measures and is referred back to during design development

This statement is intended as a succinct summary of the security requirements for the property. It forms the basis of subsequent security recommendations and, once approved, should be referred back to during design and construction.

Site-Specific Security Requirements Statement

The security requirements for University College School development are:

● To provide security features that support the marketing and operation of the development through meeting or exceeding likely guest requirements.

● To provide security that is visible and reassuring without being imposing.

● To provide a safe and secure environment for staff, guests, and assets so that the security risk to them is 'as low as reasonably practicable based on 'reasonable worst-case' security threats.

● To facilitate the management as a controlled environment, with only authorised people being granted access beyond semi-public areas.

● To provide the above against the following Design Basis Threat:

□ Multiple experienced aggressors
□ Concealable hand tools

10 Recommendations - Building Envelope and External

Recommendations are included below for consideration in the developed design, based on the established five principles of Crime Prevention through Environmental Design (CPTED); Natural surveillance, natural access control, territorial reinforcement, maintenance and activity support.

10.1 Crime Prevention through Environmental Design

Recommendations	Function
Provide suitable illumination to public areas around the building. (Dusk-till Dawn Lighting)	To provide even illumination and good colour rendition to the routes to the building.
Provide detector-activated lighting to recesses and doorways.	To provide illumination when a person enters a recess or other vulnerable area.
Consider providing clear demarcation of the extent of semi-public areas in the building. Consider using changes in colour and materials as well as signage.	To clearly indicate the boundaries of permitted public access with semi-private front-of-house and private back-of-house areas.
Display security signage at entrance points. Consider signage describing video surveillance (required), security patrols, and screening.	To clearly indicate the security measures in place around and within the building.
Provide cycle racks which are galvanised steel bar construction (minimum thickness 3mm) filled with concrete with a minimum foundation depth of 300mm with welded 'anchor bar'. To provide a level of resistance to planned or opportunist theft and to facilitate the locking of both wheels and the crossbar. To deter planned and opportunistic theft.	To provide a level of resistance to planned or opportunist theft and to facilitate the locking of both wheels and the crossbar.
To facilitate natural surveillance shrub planting should not exceed 1000 mm in height, and tree canopies should fall no lower than 2000mm from the ground.	To provide a clean and sufficient level of natural surveillance.

10.2 Video Surveillance - External

To deter crime and support the investigation of incidents in and around the development, the provision of a video surveillance system is recommended.

Cameras should be located, specified and coordinated to provide the required views, with an image resolution appropriate to the task and other performance factors such as low light performance specified to match the location and intended use.

We suggest that the industry-standard 30 days of recording time is provided for each camera in order to support post-incident investigations and to meet public expectations.

Recommendations	Function
Provide fixed external cameras viewing building entrances including the main entrance, social area entrance and along the colonnade.	To provide a view of a person entering the building.
Provide fixed external cameras viewing the pedestrian access routes to the site via external amenity spaces.	To provide a view of vehicles and pedestrians entering the site.

11 Recommendations - Landlord Areas

11.1 Physical Security

The development is likely to include operational spaces, IT rooms, plant rooms and storage rooms. Providing these spaces with tested and certified physical security products will assist in mitigating a number of security risks.

Recommendations	Function
Provide back-of-house external doors, e.g. service entrances and fire exits, with doorsets certified to LPS 1175 (noisy manual attacks) Security Rating 2 or LPS 2081 (stealth attacks) Security Rating B. If this is not possible, doorsets certified to LPS 1175 SR1 or PAS 24;2016 would provide some benefit.	LPS 1175 SR2 products provide resistance to opportunist attempts at forced entry, using bodily physical force and a range of hand tools, including those that create noise. LPS 2081 SRB products provide resistance to stealth attacks where the intruder is expected to want to avoid making significant noise.
Provide comms, IT, critical plant, valuable storage and security spaces with entrance doorsets certified to LPS 1175 SR1.	LPS 1175 SR1 provides a level of resistance to opportunist attempts at forced entry, using bodily physical force and a limited range of hand tools, including those that create noise.

11.2 Intruder Detection

To assist the local police and possible onsite security team in responding to security incidents, we recommend that an intruder and duress alarm system is provided to landlord areas. The system should include a combination of detection technologies and sensor locations that, used in tandem, serve to increase the probability of detection and minimise the false alarm rate.

Recommendations	Function
Provide an intruder alarm system to landlord areas.	To provide monitoring of alarms, reporting them to the site security control room (if provided) and local police.
Provide magnetic door contacts to doors from landlord areas to external areas and to accessible opening windows in landlord areas.	To provide an alarm when activated.
Provide volumetric detectors in landlord areas with accessible glazing or external doors (other than those that will be permanently occupied).	To provide an alarm when activated.

12 Recommendation - UCS

12.1 Physical Security - Building Envelope

The following recommendations aim to provide a suitably robust building envelope to deter and delay physical intrusion for the purposes of theft, vagrancy, or anti-social behaviour.

Specifications are aimed at meeting the design basis threats for educational use.

Recommendations	Function
All external pedestrian doors must comply with the requirements of Loss Prevention Standard 1175 Security Rating 2 (LPS1175 SR2) (or B3 under the latest classification) as a minimum.	LPS 1175 SR2 products provide resistance to opportunist attempts at forced entry, using bodily physical force and a range of hand tools, including those that create noise.
Provide laminated glass to accessible glazed areas of the building's facade. If compatible with the selected glazing system, use glass rated P1A or above under BS EN 356. If this is not possible, the laminated glazing should incorporate a PVB interlayer of a minimum thickness of 0.76mm.	To provide glazing with a degree of resistance to physical attack. P1A is the lowest rating of manual attack resistance under the BS EN 356 standard. P1A glazing is typically around 6.8mm of glass and PVB interlayer. If not possible glazing should be a minimum of 6.4mm glass and PVB interlayer.

12.2 Recommendation - Access Control

To facilitate legitimate access to and within the building and to reduce the risk of intrusion occurring through deception, tailgating, etc a layered access control system should be provided.

We suggest that a suitable access control system is specified, allowing staff to issue guest access tokens.

Recommendations	Function
Provide access control and intercom to the main entrances.	To allow management of access beyond the semi-public areas for after-hours.
Provide access control to staff-only areas e.g. staff room, separate staff-only entrance, or comms room.	To allow management of access beyond the semi-public areas.
Provide access control to doors into stairs from the ground floor.	To allow management of access to spaces above ground.
Provide access control to the door leading to the Refuse Area.	To allow management of back-of-house access.
Provide access control to doors from back of house spaces e.g. Refuse into circulation and common areas.	To allow management of staff and visitors from back-of-house areas into the building.
Consider preparing doors from landlord areas into tenant-demised areas for access control.	To enable tenants to cheaply and easily install their own access control system to their demise without additional containment etc.

13 Summary

It is concluded that security provision across all areas is proportionate to the risk with the levels of protection afforded through the physical protection elements. The additional layers of protection already within the security strategy can only serve to reinforce the physical security approach at this particular location.

With the above included, I am able to confirm that credits available under Hea06 should be claimed.

This report has been produced based on all information collated, including but not restricted to, site drawing plans and associated documents, site survey, environmental visual audit, and by subsequent correspondence. Should any amendment to the design or build specification be necessary, I should be notified in order that this security assessment can be modified as required.

Nasr Haque