GRAPHITE SECURITY

Crime Impact Statement

Maybrook House Hotel, Manchester



Figure 01 - Proposed 3D Renders (Source: JMA)

Document Control:

Report Title	Crime Impact Statement – Maybrook House Hotel, Manchester
Prepared By	Nasr Haque MSyI (SQSS) – Graphite Security Ltd
Revision	A
Date	11/05/2026
Prepared For	Deansgate Ventures Limited
Distribution	Tom McCarthy – Edmond Shipway / Deansgate Ventures Limited
Confidentiality Level	For Planning Use

1 Content

2 Executive Summary..... 5

3 Introduction..... 7

4 Positive Impacts of the Proposed Scheme..... 15

5 Crime Impact Statement: Crime Data Analysis for Maybrook House..... 18

6 Threat Identification at Maybrook House..... 23

7 Security Recommendations – Maybrook House Hotel..... 27

8 Security Recommendation - Quick Checklist:..... 44

9 Conclusion..... 50

10 Appendix A..... 52

11 Appendix B..... 53

12 Appendix C..... 56

13 Appendix D..... 61

13.1 SQSS Credentials..... 61

2 Executive Summary

This Crime Impact Statement (CIS) provides an assessment of the potential crime and security implications associated with the proposed redevelopment of Maybrook House, 40 Blackfriars Street, Manchester, M3 2EG.

The assessment considers the full application boundary and the proposed layout, comprising the refurbishment and extension of the existing building to provide a hotel-led development, with associated guest accommodation, reception/entrance areas, back-of-house spaces, servicing arrangements, plant areas, refuse provision and retained commercial/tenant interfaces at ground and lower levels.

The site is located within Manchester city centre, in the Commercial District policing neighbourhood, within an active urban environment characterised by high levels of pedestrian movement, public transport accessibility, retail, leisure, commercial, hotel and night-time economy activity. The surrounding context includes Deansgate, Blackfriars Street and Parsonage, with the site occupying a prominent corner/interface location.

The existing building currently accommodates a mix of commercial uses at ground, basement and lower levels, with upper-floor office accommodation. In its existing condition, the site presents typical city-centre risks associated with mixed-use commercial premises, including unauthorised access, opportunistic theft, anti-social behaviour, public order incidents, night-time economy spillover, and vulnerabilities associated with service entrances, refuse areas, plant spaces and shared/public-facing frontages.

The proposed development introduces a clearer hotel use and a more structured internal arrangement, with defined guest, back-of-house, service, plant and tenant zones. The ground floor includes commercial/tenant areas, back-of-house accommodation, a refuse store, BOH entrance and controlled boundary/gate arrangements, while the upper levels accommodate hotel rooms and associated support spaces.

These measures provide a strong foundation for effective security management, access control and operational supervision. However, the effectiveness of the scheme will depend on the detailed specification and implementation of key security measures, including controlled guest and staff access, secure separation between public, tenant and hotel areas, CCTV coverage, external lighting, secure door/window/glazing specifications, and appropriate management of servicing, deliveries and refuse collection.

This assessment identifies key crime risks associated with the proposed development, including unauthorised access into hotel and back-of-house areas, theft from guests or staff, anti-social behaviour at the public interface, misuse of recessed or less active areas, risks associated with servicing/refuse arrangements, and vulnerabilities linked to city-centre footfall and night-time activity. Proportionate, design-led mitigation measures are recommended to address these risks and support a safe and secure hotel environment.

Overall, subject to the implementation of the recommendations outlined within this report, the proposed development is considered capable of providing a secure, well-managed and appropriately controlled hotel environment, in accordance with Secured by Design (SBD) principles and Crime Prevention Through Environmental Design (CPTED) guidance.

3 Introduction

This Crime Impact Statement has been prepared in support of the proposed redevelopment of Maybrook House, 40 Blackfriars Street, Manchester, M3 2EG. This report provides an assessment of the potential crime and security risks associated with the scheme and sets out proportionate, design-led measures to address these risks.

The proposed development comprises the refurbishment and extension of the existing building to provide a hotel-led scheme, with associated guest accommodation, reception/entrance areas, back-of-house accommodation, servicing arrangements, plant areas, refuse provision and retained commercial/tenant interfaces at lower levels.

Given the city-centre location and the proposed hotel use, security considerations are important in ensuring a safe, well-managed and appropriately controlled environment for guests, staff, visitors, commercial tenants and servicing activity.

3.1 Background

The site is located within Manchester city centre, at the junction/interface of Blackfriars Street, Deansgate and Parsonage, within the Commercial District policing neighbourhood. The surrounding area is characterised by a mix of commercial, hospitality, leisure, retail, office, transport and night-time economy uses, with high levels of pedestrian and vehicular movement.

The existing building currently accommodates a mix of commercial uses at the basement, ground and lower levels, with upper-floor office accommodation. The Design and Access Statement identifies existing uses including Tesco, a coffee shop, travel agent and basement bar, with restaurant use at first floor and offices above.

The proposed scheme seeks to reposition the building through refurbishment, extension and conversion to hotel use. The area schedule identifies a hotel scheme of 238 keys, comprising 226 standard rooms and 12 accessible rooms.

As such, the security context is influenced by the site's central location, public accessibility, active street frontages, retained commercial interfaces, guest access arrangements, back-of-house activity and servicing requirements. Key considerations include the control of access, separation between public, tenant, guest and staff-only areas, and the management of risks associated with city-centre footfall and night-time activity.

3.2 Purpose

The purpose of this Crime Impact Statement is to:

Evaluate the Proposed Design
Assess the proposed layout, access arrangements, internal zoning and building configuration to identify key strengths and any areas requiring improvement in relation to security.

Identify and Mitigate Potential Risks
Identify potential opportunities for crime, disorder and unauthorised activity arising from the design and operational context, and provide proportionate mitigation measures to reduce these risks and support a secure hotel environment.

3.3 Scope

This assessment considers the following key aspects of the development:

Physical Security
Review of the building layout, entrances, back-of-house areas, refuse store, plant areas, roof/plant access, doors, windows, glazing and other accessible or vulnerable elements.

Access and Movement
Assessment of pedestrian, guest, staff, tenant, servicing and back-of-house access arrangements, including the separation and control of public, semi-private and restricted areas.

Territoriality
Evaluation of how clearly the development defines public, tenant, guest-only, staff-only and back-of-house areas, including the transition between the public highway and controlled hotel areas.

Management and Operation
Consideration of how ongoing hotel management, staff procedures, CCTV monitoring, access control, deliveries, refuse collection and maintenance arrangements will support security and reduce opportunities for unauthorised access or misuse.

3.4 Development Overview and Extent of Assessment

The proposed development comprises the refurbishment and extension of Maybrook House to provide a hotel-led development within the application boundary, with retained commercial/tenant interfaces and associated back-of-house and servicing functions.

For the avoidance of doubt, this CIS considers the development as a whole, including:

- Guest entrance and reception/access arrangements;
- Hotel rooms and upper-floor guest corridors;
- Lift lobbies, stair cores and circulation areas;
- Back-of-house areas, staff/service access and BOH entrance points;
- Refuse store and servicing arrangements;
- Basement and plant areas, including substation, comms, switchroom, tank rooms and AHU spaces;
- Commercial/tenant interfaces at ground and lower levels;
- Roof and upper-level plant/access areas;
- External frontage interfaces with Blackfriars Street, Deansgate and Parsonage;
- Boundary/gate arrangements shown at ground level;
- Transitions between public realm, tenant areas, hotel guest areas and restricted operational space.

The ground-floor plan identifies BOH areas, escape stairs, BOH lift, refuse store, BOH entrance, existing tenant areas and an extended fence with proposed gates to match the existing fence. The basement plan includes plant, substation, comms, switchroom, sprinkler tank, CWS tank and AHU-related accommodation.

3.5 Methodology

This assessment has been undertaken using a structured approach, including:

- Review of the available architectural drawings, area schedule and design information;
- Consideration of the site context and surrounding city-centre land uses;
- Review of the proposed access, servicing, back-of-house and operational arrangements;
- Consideration of the relevant crime and disorder context for the Commercial District policing neighbourhood;
- Application of established crime prevention principles and best practice guidance.

The assessment is informed by the principles of Crime Prevention Through Environmental Design (CPTED) and Secured by Design (SBD). Relevant concepts from ISO 22341 have also been considered where appropriate.

Where design constraints exist due to the retained building, city-centre location or existing commercial interfaces, proportionate and practical mitigation measures are identified to ensure that an appropriate level of security can be achieved.

3.6 Visual Audit - Site Survey

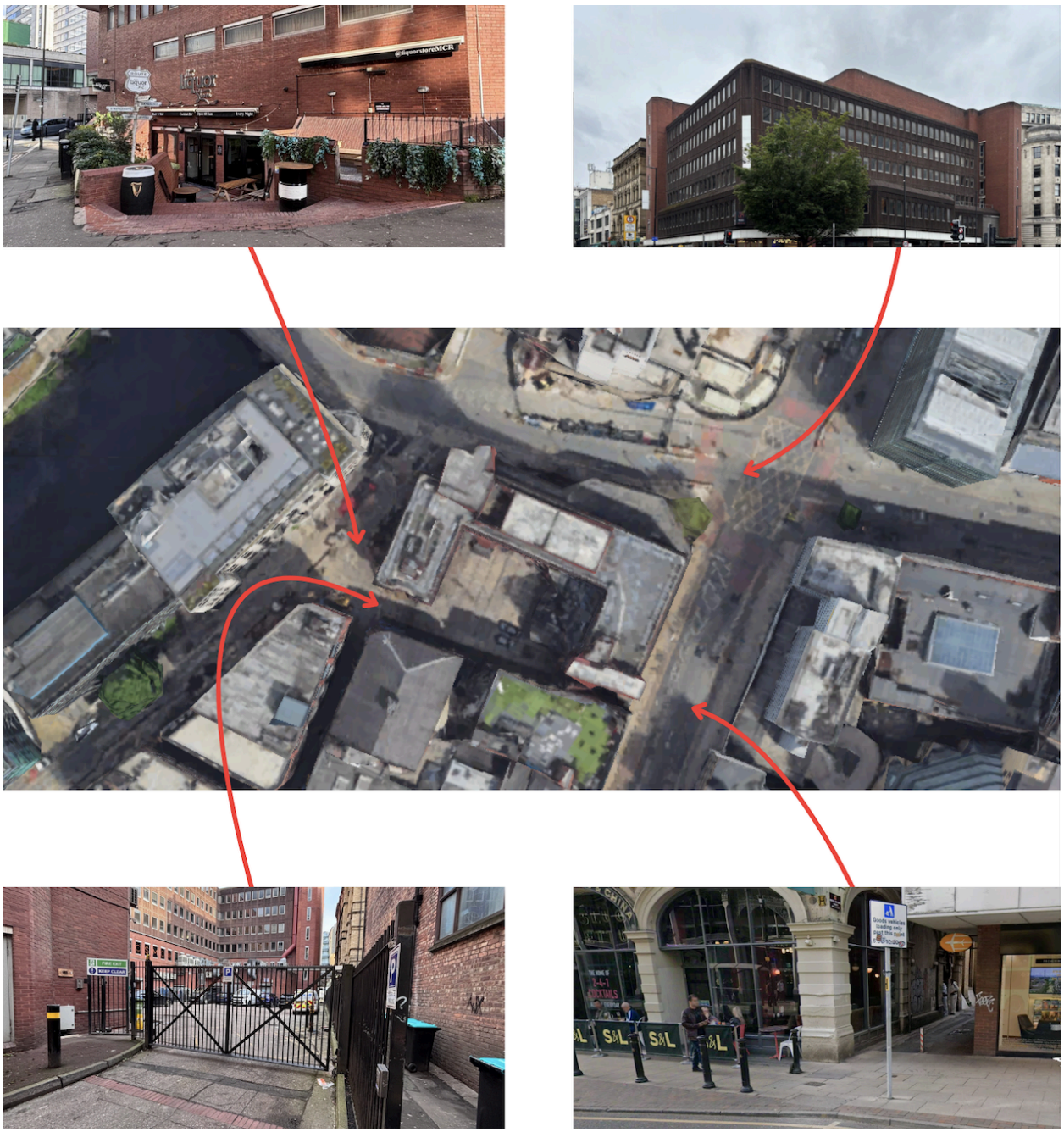


Figure 02 - Site Survey (Source: Graphite Security Ltd & Google Maps)

3.7 Enhancing Security Through Layered Design

Security within the development should be delivered through a coordinated and layered approach, combining physical design measures with appropriate hotel management and operational controls.

Public Realm Interface
The development fronts onto a busy city-centre environment. Frontage design, lighting, visibility and entrance management should support legitimate use while discouraging loitering, concealment and unauthorised access.

Access Control
Guest, staff, tenant and servicing access should be clearly separated and controlled. Access into guest-room floors, BOH areas, plant rooms, roof areas and service zones should be restricted to authorised users only.

Natural Surveillance
The proposed layout should maximise visibility across entrances, reception/guest arrival points, commercial frontages, BOH access points and refuse/service areas. Avoidance of unmanaged recessed spaces will be important.

Lighting
External lighting should be designed to ensure all entrances, service points, frontage areas and vulnerable external interfaces are appropriately illuminated, while avoiding glare or nuisance to neighbouring uses.

Physical Security Measures
Appropriate security standards should be applied to accessible doors, windows, glazing, service entrances, plant rooms, comms rooms, roof access and BOH areas. This is particularly important given the city-centre location and the public-facing nature of the building.

Servicing, Refuse and BOH Areas
Back-of-house, refuse, and servicing areas should be secure, access-controlled, well-lit, monitored where appropriate and managed to prevent tailgating, concealment or unauthorised access into the hotel.

Management and Operation
Ongoing management and operational procedures are critical to maintaining site security, including reception procedures, visitor management, staff training, CCTV monitoring, incident reporting, deliveries, refuse collection and maintenance of security infrastructure.

A coordinated approach ensures that security is delivered through a combination of design, specification, management and operational control.

3.8 Importance

The safety and security of the development, its guests, staff, visitors, commercial tenants and surrounding users are key considerations within the design and management of the scheme. This Crime Impact Statement supports the integration of crime prevention principles into the proposed redevelopment, ensuring that security is embedded within the layout, access strategy and operational arrangements.

By identifying potential risks and providing proportionate mitigation measures, the development can deliver a safe, secure and well-managed hotel environment, consistent with the principles of Secured by Design and CPTED.

4 Positive Impacts of the Proposed Scheme

The proposed redevelopment of Maybrook House, 40 Blackfriars Street, Manchester, M3 2EG, is expected to deliver a number of positive outcomes in terms of building security, access control, operational management and overall safety. The scheme refurbishes and repositions an existing city-centre building to provide a hotel-led development, with clearer internal zoning, upgraded frontages and improved management of guest, staff, tenant and servicing areas.

Enhanced Surveillance and Activity

The proposed hotel use will introduce consistent levels of activity throughout the day and evening, including guest arrivals and departures, staff presence, reception activity, servicing operations and routine management oversight. This increased occupation and activity will support improved levels of natural surveillance across key areas of the building, including entrances, frontages, lift lobbies, circulation routes and back-of-house access points.

The retained and proposed commercial interfaces at lower levels will also contribute to street-level activation, helping to maintain passive surveillance and legitimate activity around the public-facing edges of the building.

Improved Building Definition and Control

The proposed layout creates a clearer distinction between public, tenant, guest-only, staff-only and back-of-house areas. This is important within a city-centre hotel environment, where the public-facing nature of the building must be balanced with the need to prevent unauthorised access into guest accommodation, service areas, plant rooms and restricted operational spaces.

The ground-floor plan identifies BOH areas, refuse store, BOH entrance, existing tenant interfaces and proposed gated boundary treatment, providing

opportunities to strengthen access control and territorial definition at key operational points.

Controlled Access and Managed Permeability

The development provides an opportunity to implement a controlled access strategy across the building. This should include clear separation between guest access, tenant access, staff/service access, refuse collection, plant access and emergency escape routes.

Where properly specified and managed, controlled permeability will allow the hotel to operate efficiently while reducing opportunities for tailgating, unauthorised entry, theft, misuse of circulation areas or access into restricted parts of the building.

Structured Hotel Layout and Internal Zoning

The proposed upper-floor layouts provide a structured arrangement of hotel rooms, lift lobbies, circulation areas, housekeeping spaces, IT/electrical rooms, risers and support accommodation. This provides a good basis for applying layered security controls, including access-controlled lift/stair movement, restricted staff-only areas and clear separation between guest and operational spaces.

The area schedule identifies a hotel scheme of 238 keys, comprising 226 standard rooms and 12 accessible rooms, which reinforces the need for a clear operational security strategy to support guest safety, staff supervision and controlled building management.

Lighting and Environmental Improvements

The redevelopment provides an opportunity to implement a coordinated lighting strategy across the building's external interfaces, entrances, BOH/service areas, refuse store, escape routes and any recessed or less active spaces. Appropriate lighting will enhance visibility, support CCTV performance, assist

legitimate users and reduce opportunities for concealment or anti-social behaviour.

The proposed façade and frontage improvements will also improve the building's appearance and presence within the street scene, supporting a more active, cared-for and professionally managed environment.

Activation of an Existing City-Centre Building

The redevelopment will bring the existing building into a more active and managed hotel use, replacing upper-floor office accommodation with hotel use while working alongside retained lower-level commercial interfaces. This is likely to improve overall building stewardship, increase routine management presence and reduce risks associated with poorly supervised or ambiguous internal areas.

The Design and Access Statement identifies the site as occupying a central location with strong public transport accessibility and proximity to Exchange Square, Victoria Station and surrounding commercial/leisure destinations. This context supports the suitability of an active, well-managed hotel use, provided that the necessary access control and operational security measures are embedded into the design.

Overall Impact

The proposed scheme has the potential to deliver a clear improvement in terms of building security, access control, natural surveillance and operational management. Through the introduction of defined access arrangements, improved internal zoning, active hotel occupation and upgraded frontages, the development can create a safer and more secure city-centre hotel environment.

These benefits are, however, dependent on the effective specification and implementation of appropriate security measures, as outlined within this report.

5 Crime Impact Statement: Crime Data Analysis for Maybrook House

5.1 Executive Summary

This assessment considers crime data and local context relevant to the proposed redevelopment of Maybrook House, 40 Blackfriars Street, Manchester, M3 2EG.

The site falls within the Commercial District policing neighbourhood under Greater Manchester Police (GMP). The purpose of this analysis is to provide a proportionate understanding of local crime patterns and how these may influence the proposed hotel-led development.

The data has been considered in the context of the surrounding environment, which comprises a mix of commercial, retail, hospitality, leisure, office, transport and night-time economy uses. This city-centre context is relevant to the proposed hotel use, particularly in relation to public accessibility, guest movement, servicing activity, and the need to control access between public, guest-only and staff-only areas.

It is acknowledged that Police.uk data is anonymised and generalised, meaning it does not represent precise incident locations. Police.uk also notes that its crime map hotspots provide only a loose indication of where crimes occurred and that actual locations and details of crimes are kept anonymous.

It should also be noted that Greater Manchester Police has not consistently provided crime data to Police.uk / data.police.uk for several years. The data.police.uk changelog records repeated entries stating that "Greater Manchester Police: Crime data not provided", including multiple recent monthly reporting periods in 2025.

Due to this limitation, this assessment has not relied solely on the current Police.uk crime mapping. Older available Police.uk data, GMP's own published neighbourhood crime data, and the wider Manchester city-centre context have been used to inform a proportionate assessment. GMP publishes neighbourhood crime tables showing recorded neighbourhood crimes between 2019 and 2026.

5.2 Source of Crime Data

The primary crime data sources for this assessment are Police.uk / data.police.uk information for the Commercial District policing neighbourhood and Greater Manchester Police's own published neighbourhood crime data.

This has been supplemented by an understanding of the local context, including city-centre land use, pedestrian movement, hospitality and leisure activity, transport accessibility, servicing requirements and the operational characteristics of hotel developments.

Due to the known limitations of the current Police.uk data for Greater Manchester, the crime data has been interpreted proportionately and should be read as an indication of broader local patterns rather than a precise record of incidents at, or immediately adjacent to, the site.

Screenshots and/or references to the relevant crime data sources are provided within Appendix A for reference.

5.3 Local Area Context and Crime Profile

Crime data and local context indicate a profile typical of a busy city-centre commercial area, with reported offences influenced by high footfall, public accessibility, retail and hospitality activity, transport movement and the night-time economy.

The most relevant offences for the proposed hotel development are considered to include violence and public order, theft-related offences, anti-social behaviour, vehicle-related crime, and criminal damage/arson.

Whilst violence and public order offences represent important considerations within the wider city-centre context, they are generally associated with public interaction, evening activity and the wider street environment. For the proposed hotel, these risks are most relevant to guest arrival and departure, reception management, external frontages, staff procedures and the need for clear visibility and oversight at public-facing entrances.

Of greater direct relevance to the proposed development are the following:

Theft and Opportunistic Crime
The presence of hotel guests, luggage, personal belongings, staff areas, deliveries and public-facing reception spaces creates potential opportunities for theft and opportunistic crime. This is particularly relevant to entrance areas, reception, guest circulation routes, back-of-house areas and any service routes that are not clearly controlled.

Anti-Social Behaviour and Public Order
Anti-social behaviour and public order incidents can occur in busy city-centre areas, particularly where there is high footfall, night-time activity, recessed spaces, unclear ownership or limited surveillance. This is relevant to the hotel entrance, external frontages, service areas, refuse areas and less active edges of the building.

Vehicle-Related Crime
Although the development does not appear to include significant dedicated guest parking, vehicle-related crime remains relevant due to taxis, drop-off and pick-up activity, servicing vehicles, staff travel and nearby public car parks. Guests may also use nearby parking facilities and walk to and from the hotel.

Criminal Damage and Arson
Criminal damage is typically associated with vulnerable or poorly supervised external features. For this development, external doors, glazing, signage, service entrances, refuse areas, plant interfaces and louvred areas may require appropriate protection, lighting, management and surveillance. Refuse storage should be secure and controlled to reduce misuse and arson risk.

Unauthorised Access
Unauthorised access is a key consideration for the proposed hotel use. The building includes public-facing areas, commercial/tenant interfaces, guest accommodation, back-of-house spaces, refuse provision, plant areas and roof/plant access. Clear zoning and access control will therefore be important to prevent public access into guest-only, staff-only and operational areas.

5.4 Data Analysis Methodology

The crime data assessment has been undertaken through a review of available information for the Commercial District policing neighbourhood, focusing on:

The frequency and nature of crime types relevant to a city-centre hotel environment;

- Identification of recurring crime and disorder patterns associated with commercial, hospitality and night-time economy areas;
- Consideration of how local context, land use, pedestrian movement and operational activity influence crime risk;
- Consideration of the known limitations with current GMP data on Police.uk / data.police.uk.

This approach provides a proportionate understanding of crime risk without over-reliance on incomplete current Police.uk street-level data, ensuring that conclusions are relevant to the nature and setting of the proposed development.

5.5 Appendices

Appendix A: Available Police.uk / data.police.uk information for the Commercial District policing neighbourhood, including a note on GMP data limitations.

Appendix B: Greater Manchester Police neighbourhood crime data reference, where available.

These include, where available:

- Overview of relevant crime types;
- Available older Police.uk / data.police.uk information;
- GMP neighbourhood crime data references;
- Commentary on data limitations and interpretation.

5.6 Conclusion

The crime data analysis indicates that the site is located within a busy city-centre environment experiencing crime types typical of a commercial and hospitality area, including theft-related offences, anti-social behaviour, public order incidents, vehicle-related offences, criminal damage/arson and unauthorised access risks.

These risks are primarily influenced by public accessibility, high pedestrian footfall, nearby commercial and leisure activity, night-time economy influence, and the need to clearly separate public areas from guest-only and staff-only hotel spaces.

The proposed hotel redevelopment has the potential to positively influence these conditions through the introduction of a controlled and actively managed building, improved internal zoning, reception oversight, enhanced access control, lighting, CCTV and secure back-of-house arrangements.

However, the effectiveness of this will depend on the implementation of appropriate security measures, particularly in relation to entrance control, guest-floor access, back-of-house security, refuse and servicing arrangements, plant-room protection, external lighting, CCTV and operational management procedures.

6 Threat Identification at Maybrook House

6.1 Overview

The identification of site-specific threats is essential in informing proportionate and effective security measures. This section considers the primary risks associated with the proposed redevelopment of Maybrook House, 40 Blackfriars Street, Manchester, informed by available crime data, the known limitations of the current Police.uk data for Greater Manchester, the city-centre context, and a review of the proposed hotel-led layout.

The scheme comprises a hotel-led redevelopment with associated guest accommodation, reception/entrance areas, commercial/tenant interfaces, back-of-house spaces, refuse provision, plant areas and servicing arrangements. Whilst the layout provides opportunities for clear zoning and controlled access, a number of vulnerabilities remain, particularly in relation to public-facing entrances, guest access, back-of-house control, refuse areas and plant spaces.

6.2 Key Threats Identified

Unauthorised Access
Unauthorised access represents a key risk due to the presence of public-facing areas, guest accommodation, commercial/tenant interfaces, staff-only spaces, back-of-house areas and plant rooms. Without appropriate control measures, there is potential for unauthorised movement into guest corridors, staff areas, service spaces, plant rooms or roof/plant areas.

Theft and Opportunistic Crime
Hotel environments can attract opportunistic theft due to the presence of guests, luggage, personal belongings, deliveries, staff facilities and public-facing reception spaces. Risks are particularly associated with entrances, reception areas, guest circulation, back-of-house spaces and service routes where access control or surveillance may be limited.

Anti-Social Behaviour and Public Order
Given the city-centre location and surrounding commercial, leisure and night-time economy uses, anti-social behaviour and public order incidents may occur within the wider area. These risks are relevant to the hotel frontage, entrance points, external gathering areas, staff safety and guest arrival/departure.

Vehicle-Related Crime
Although the scheme does not appear to include extensive dedicated guest parking, vehicle-related crime remains relevant due to taxi/drop-off activity, servicing vehicles, staff travel, nearby streets and surrounding public car parks. This risk is particularly relevant to guest and staff movement to and from the hotel.

Criminal Damage and Arson
External areas, including doors, glazing, signage, refuse storage, service entrances, plant interfaces and less active frontages, may be vulnerable to criminal damage or misuse where surveillance is limited or access is not adequately controlled. Refuse storage areas should be secure and managed to reduce the risk of arson or deliberate misuse.

6.3 Contributing Factors

The identified threats are influenced by a number of site-specific factors:

Public-Facing City-Centre Location
The site is located within a busy city-centre commercial district with high levels of pedestrian movement, visitor activity and evening/night-time use. This increases exposure to opportunistic crime, anti-social behaviour and public order issues.

Hotel Use and Guest Movement
Hotels require a degree of public accessibility, particularly at entrances and reception areas. This creates a need for careful management and access control to prevent unauthorised movement from public areas into guest-only or staff-only zones.

Mixed Tenant and Operational Interfaces
The presence of commercial/tenant interfaces at lower levels creates a need for clear separation between tenant areas, hotel areas, back-of-house spaces and guest circulation routes.

Back-of-House, Refuse and Servicing Areas
Back-of-house, refuse, and servicing areas may be vulnerable where they are less visible, poorly lit or not access-controlled. These areas may also provide opportunities for tailgating, concealment or unauthorised access into operational areas if not properly designed and managed.

Plant and Roof Access
Plant rooms, comms rooms, risers, service areas and roof/plant spaces require restricted access to prevent tampering, theft, damage or unauthorised entry.

Lighting and Visibility
Inadequate lighting can increase the risk of crime by creating poorly overlooked or concealed areas, particularly at entrances, external frontages, service points, and refuse areas.

6.4 Threat Assessment Methodology

The identification of threats has been informed by a review of available crime data, combined with an assessment of the site layout, access arrangements, surrounding city-centre context and proposed hotel use.

Due to the known limitations with current GMP data on Police.uk / data.police.uk, the assessment has also considered older available Police.uk information, GMP's own published neighbourhood crime data, and the wider local context.

This approach ensures that both local crime patterns and site-specific operational risks are considered, allowing for a proportionate and targeted assessment.

6.5 Conclusion

The primary risks associated with the proposed development relate to unauthorised access, theft and opportunistic crime, anti-social behaviour/public order, vehicle-related crime, and criminal damage/arson.

These risks are typical of a busy city-centre hotel environment and are largely influenced by public accessibility, high footfall, night-time activity, mixed-use surroundings, and the need to control movement between public, guest, tenant and staff-only areas.

The proposed scheme has the potential to mitigate these risks through the implementation of a clear access control strategy, secure internal zoning, effective CCTV coverage, appropriate lighting, reception oversight, secure back-of-house/refuse arrangements, restricted plant access and robust operational procedures.

Subject to the implementation of the recommendations outlined within this report, the development is capable of delivering a secure and well-managed hotel environment.

7 Security Recommendations – Maybrook House Hotel

7.1 Overview

The proposed redevelopment comprises the refurbishment and extension of Maybrook House to provide a hotel-led development within Manchester city centre. The scheme includes guest accommodation, a guest entrance, lift/stair cores, public and back-of-house areas, commercial/tenant interfaces, refuse provision, plant rooms, service areas and roof-level plant access.

This section sets out the recommended Security and Operational Strategy for the development. It has been prepared to support the Crime Impact Statement and to address the key security matters typically expected by the Local Authority and Police Designing Out Crime Officer for a city-centre hotel development.

The strategy focuses on:

- Controlled access to the hotel entrance, guest floors and staff-only areas;
- Clear separation between public, guest, tenant and back-of-house areas;
- Protection of lift lobbies, stair cores and circulation routes;
- Security of back-of-house, refuse, plant, comms and service areas;
- Management of lower ground, ground floor and public-facing entrances;
- CCTV coverage and lighting to key entrances, routes and vulnerable areas;
- Protection of accessible doors, glazing, windows and service entrances;
- Management procedures for guests, visitors, staff, deliveries and refuse collection.

The proposed layout already includes positive security features, including a defined guest entrance, back-of-house areas, refuse store, BOH entrance, existing tenant interfaces, lift/stair cores and proposed gated boundary treatment. These features provide a suitable foundation for a secure hotel development, subject to detailed specification, access control and operational management.

7.2 Guest Entrance, Reception and Front-of-House Control

🟥 **Mandatory**

The guest entrance and any associated reception / front-of-house area should operate as the primary controlled threshold between the public realm and the hotel.

The guest entrance should be:

- Clearly identifiable from the public realm;
- Well-lit and naturally visible;
- Covered by CCTV;
- Designed to avoid unnecessary recesses or concealment points;
- Supported by reception or staff oversight where practicable;
- Capable of being controlled during late evening and overnight periods;
- Designed to prevent unauthorised movement beyond the public/reception area.

Access from the guest entrance/reception area into guest accommodation floors should be controlled. Members of the public should not be able to move freely from the entrance or reception area into guest corridors, stair cores, lifts, back-of-house areas or plant spaces.

Where lift access is available from public-facing areas, lift controls should be linked to room keys, staff cards, fobs or other suitable access control systems, so that guests can only access authorised floors and staff-only areas remain restricted.

Why this is important:

The site is located in a busy city-centre environment with high pedestrian movement and night-time activity. A clearly managed hotel entrance reduces opportunities for unauthorised access, tailgating, theft, anti-social behaviour and movement into guest-only or staff-only areas.

7.3 Lift, Stair Core and Guest Floor Access Control

🟥 **Mandatory**

The hotel lift and stair core strategy should be designed to prevent unauthorised access to guest accommodation floors, back-of-house areas, plant rooms and roof/plant areas.

Lift and stair access should be controlled so that:

- Guest lifts do not allow unrestricted access from public areas to all hotel floors;
- Guest access is restricted to authorised floors only, where practicable;
- Staff/service lifts are separated from public or guest use where operationally possible;
- Stair cores do not provide uncontrolled access from the public realm or lower levels to guest floors;
- Emergency escape requirements are maintained without compromising security;
- Roof, plant and service levels are restricted to authorised staff and contractors only.

Where escape stairs discharge to the public realm or external areas, the final exit doors should be designed to prevent unauthorised re-entry, while remaining fully compliant with fire safety and means of escape requirements.

Why this is important:

The drawings identify lift lobbies, service lift arrangements, stair cores and upper-floor guest accommodation. These vertical circulation routes are key security control points. If lifts or stairs are not appropriately managed, they can provide direct access to guest corridors, staff areas, roof spaces or plant rooms.

7.4 Separation of Hotel, Tenant and Back-of-House Areas

🟥 **Mandatory**

The development includes existing/proposed commercial or tenant interfaces at lower levels, alongside hotel guest and back-of-house functions. A clear separation strategy must be maintained between:

- Public areas;
- Commercial/tenant areas;
- Hotel guest areas;
- Staff-only areas;
- Back-of-house/service areas;
- Plant, comms and technical spaces;
- Refuse and servicing areas.

Internal doors between tenant, hotel, back-of-house and guest areas should be access-controlled or secured to prevent unauthorised movement between uses.

Any shared corridors, service routes or interfaces should be reviewed at the detailed design stage to ensure that public or tenant users cannot gain access to hotel guest floors, staff areas, service lifts, plant rooms, or refuse areas.

Why this is important:

Mixed-use buildings can create vulnerabilities where different users share entrances, corridors, lifts or service routes. Clear separation reduces the risk of unauthorised access, theft, staff vulnerability and movement into areas not intended for public use.

7.5 Back-of-House, BOH Entrance and Service Access

🟥 **Mandatory**

Back-of-house areas, including the BOH entrance, service routes, staff areas, goods lift and support spaces, should be treated as restricted operational areas.

BOH entrances should be:

- Access-controlled;
- Self-closing and self-locking;
- Well-lit;
- Covered by CCTV where practicable;
- Clearly separated from guest/public access routes;
- Designed to prevent tailgating;
- Managed through staff procedures.

Service access and delivery arrangements should be controlled through agreed operational procedures. Deliveries should be booked, supervised or verified by staff, and delivery personnel should not be able to move freely into guest accommodation areas or unrestricted back-of-house spaces.

Where goods lifts are used, access should be controlled so that they cannot be used by unauthorised persons to access guest floors, basement areas, plant rooms or other restricted parts of the building.

Why this is important:

Back-of-house entrances and service routes are common vulnerabilities in hotel and mixed-use buildings. They may be used by staff, contractors, cleaners, deliveries and refuse collectors, and therefore require clear access control and management to prevent unauthorised entry.

7.6 Refuse Store and Waste Management Security

🟥 **Mandatory**

The refuse store should be secure, well-managed and integrated into the wider access control strategy.

The refuse store should be:

- Robustly constructed;
- Access-controlled or lockable;
- Located away from vulnerable openings where practicable;
- Well-lit;
- Covered by CCTV or passive surveillance where appropriate;
- Managed to prevent misuse, rough sleeping, concealment or arson risk;
- Kept closed and secured when not actively in use.

Waste collection arrangements should be managed so that refuse collection does not create an uncontrolled access route into back-of-house or hotel areas.

Why this is important:

Refuse stores can attract misuse, anti-social behaviour, concealment and arson risk if poorly secured. In a city-centre hotel environment, refuse areas should not provide an opportunity for unauthorised access into service or back-of-house spaces.

7.7 Basement, Plant, Substation and Comms Room Security

🟥 **Mandatory**

Basement and plant areas, including the plant entrance, substation, comms room, AHU, switchroom, sprinkler tank room, CWS tank room and associated technical spaces, should be treated as restricted access areas.

These areas should be:

- Secured against unauthorised access;
- Clearly marked as restricted/staff-only where appropriate;
- Access-controlled or lockable;
- Protected by suitable door and lock specifications;
- Covered by CCTV or alarm detection where proportionate;
- Subject to contractor and maintenance access procedures;
- Kept separate from guest and public circulation routes.
- Plant rooms, comms rooms and switchrooms should not be accessible from guest or public areas without staff authorisation.

Why this is important:

Plant, comms, electrical and water infrastructure are critical to hotel operation. Unauthorised access could create risks of theft, tampering, disruption, damage, arson or wider building safety issues.

7.8 Roof, 8th Floor Plant and Access Hatch Security

🟥 Mandatory

Roof-level and upper plant areas, including the 8th floor plant/access hatch, AHU, ASHP compound, switchroom, PV zone, AOVs and smoke fan areas, should be restricted to authorised staff and contractors only.

Roof and plant access should be:

- Access-controlled or locked;
- Clearly restricted to authorised personnel;
- Covered by staff/contractor access procedures;
- Designed to prevent unauthorised climbing or access from guest areas;
- Protected from tampering, theft or damage;
- Reviewed to ensure no accessible route is created from adjoining roofs, terraces, ledges or plant structures.
- Any access hatch should be secured with a suitable lock or access control arrangement and should not be accessible to guests or the public.

Why this is important:

Roof and plant areas can present risks of unauthorised access, trespass, tampering, theft of equipment and disruption to building services.

7.9 Doors, Windows and Accessible Glazing

🟥 Mandatory

All accessible external doors, service doors, BOH doors, plant room doors and doors leading to restricted areas should be specified to an appropriate security standard.

The final door and security specification should be confirmed by the architect/design team to ensure that the proposed standards are appropriate and achievable for the retained building, external doors, BOH doors and tenant interfaces.

External and vulnerable doors should meet one of the following recognised standards, as appropriate to location and risk:

- LPS 1175 SR2 (B3);
- STS 202 BR2;
- LPS 2081 SR B;
- BS EN 1627 RC3;
- PAS 24:2022, where appropriate.

Accessible windows and glazing at ground floor, lower ground, vulnerable elevations, service areas or locations reachable from the public realm should be specified to resist opportunistic attack.

Accessible glazing should include laminated glass to a suitable standard, with consideration given to BS EN 356 P1A as a minimum for accessible or vulnerable locations, subject to the final façade and glazing specification.

Doors should include:

- Secure locking;
- Robust frames and ironmongery;
- Self-closing arrangements where required;
- Anti-tailgating control where relevant;
- Protection against manipulation or forced entry;
- Compatibility with fire escape requirements.

Why this is important:

The building includes public-facing frontages, glazed doors, service doors, plant/service areas and commercial interfaces. Door and glazing specifications are therefore important to reduce risks of burglary, unauthorised access, vandalism and opportunistic entry.

7.10 CCTV Strategy

🟥 Mandatory

A CCTV system should be provided to support deterrence, monitoring and post-incident investigation.

CCTV should cover, as a minimum:

- Main guest entrance;
- Reception / front-of-house area;
- Public-facing entrance points;
- BOH entrance and service access;
- Refuse store access;
- Lift lobby areas where appropriate;
- Stair core access points where appropriate;
- Commercial/tenant interface points where relevant;
- Basement/plant access points;
- Roof/plant access points where appropriate;
- External frontage areas and any recessed or less active spaces;
- Areas where guests, staff or visitors may be vulnerable.

The CCTV system should be designed in accordance with BS EN 62676 and installed by a suitably competent contractor, preferably NSI or SSAIB accredited.

Cameras should be positioned to avoid blind spots and should be supported by appropriate lighting to ensure usable images during hours of darkness.

CCTV signage and data handling procedures should comply with relevant data protection requirements.

Why this is important:

CCTV provides a deterrent and supports investigation following incidents. It is particularly important in a city-centre hotel where public access, guest movement, servicing, night-time activity and back-of-house access all require monitoring.

7.11 External Lighting Strategy

🟥 **Mandatory**

A coordinated external lighting strategy should be implemented across the development.

Lighting should cover:

- Guest entrance;
- Public-facing frontage areas;
- BOH entrance;
- Refuse store access;
- Service routes;
- External escape doors;
- Basement/plant access points;
- Commercial/tenant interfaces where relevant;
- Any recessed or less active areas around the building;
- External areas supporting CCTV coverage.

Lighting should comply with BS 5489:2020 and should be designed to provide consistent illumination without creating glare, excessive light spill or dark recesses.

Lighting should support CCTV performance and allow safe movement of guests, staff, visitors, contractors and servicing personnel.

🟥 Mandatory Note:

Decorative or low-level lighting alone should not be relied upon for security-critical areas such as entrances, BOH access points, refuse areas, service routes and plant access points.

Why this is important:

Good lighting supports natural surveillance, improves personal safety, assists CCTV performance and reduces concealment opportunities. This is particularly important given the city-centre location and potential evening/night-time use.

7.12 Secluded Areas, Recesses and Public Realm Interface

🟥 **Mandatory**

The building frontage and external edges should be designed and managed to avoid creating unnecessary concealment, loitering or anti-social behaviour opportunities.

Particular attention should be given to:

- Entrance recesses;
- BOH and service entrances;
- Refuse store access;
- Escape doors;
- Less active elevations;
- Areas around proposed gates/fencing;
- Corners or setback areas where visibility may be reduced.
- Where recessed areas cannot be avoided, they should be:
- Well-lit;
- Covered by CCTV where appropriate;
- Clearly defined as part of the managed building;
- Designed to avoid seating/loitering opportunities unless intentionally managed;
- Subject to routine staff inspection and management.

Why this is important:

City-centre buildings can be vulnerable to anti-social behaviour, rough sleeping, concealment and opportunistic crime where inactive or recessed spaces are created. The design should support clear visibility, ownership and active management.

7.13 Guest Room Floors, Corridors and Housekeeping Areas

🟥 **Mandatory**

Guest accommodation floors should be managed as controlled zones.

Guest room corridors, housekeeping areas, risers and staff/service cupboards should be:

- Accessible only to authorised guests and staff;
- Separated from public/tenant areas;
- Supported by controlled lift/stair access;
- Covered by appropriate staff procedures;
- Secured where they contain plant, services, cleaning materials or operational equipment.
- Housekeeping stores, IT/electrical rooms, risers and service cupboards should be lockable and restricted to authorised staff only.

Why this is important:

Hotel room floors contain guests, personal belongings and staff operational areas. Controlling access to corridors, housekeeping spaces and service risers reduces risks of theft, unauthorised entry, tampering and guest safety incidents.

7.14 Signage, Wayfinding and Territorial Definition

🟦 Advisory

Clear signage and wayfinding should be used to support legitimate movement and reinforce territorial control.

Signage should clearly identify:

- Hotel entrance;
- Reception;
- Staff-only areas;
- Tenant/commercial areas;
- Emergency exits;
- Restricted plant/service areas;
- Refuse and servicing access where required.

Staff-only and back-of-house areas should not appear open or ambiguous to members of the public. Restricted areas should be clearly defined without creating an unnecessarily defensive appearance.

Why this is important:

Clear signage reduces confusion and helps prevent members of the public, guests or contractors from entering areas not intended for them. It also supports staff challenge and operational control.

7.15 Operational Hotel Management Procedures

🟥 **Mandatory**

Security should be supported by clear operational procedures.

The hotel operator should develop and implement procedures covering:

- Guest check-in and reception control;
- Late-night entrance management;
- Visitor management;
- Staff access control;
- Key card/fob management;
- Contractor sign-in and supervision;
- Delivery booking and verification;
- Refuse collection procedures;
- BOH access control;
- Plant and roof access procedures;
- CCTV monitoring and incident review;
- Reporting of suspicious activity;
- Management of anti-social behaviour at entrances/frontages;
- Emergency escalation procedures;
- Routine inspections of doors, lighting, CCTV and access control systems.

A clear distinction should be maintained between:

- Public areas;
- Commercial/tenant areas;
- Guest-only areas;
- Staff-only areas;
- Back-of-house areas;
- Plant and roof access areas.

Why this is important:

Physical security measures are only effective where supported by good management. Hotel security relies on staff awareness, access control, CCTV monitoring, visitor management and consistent operational procedures.

7.16 Maintenance and Management

🟦 **Advisory**

The development should be maintained to ensure that security measures remain effective over time.

This should include regular checks of:

- Access control equipment;
- Guest and staff entrance doors;
- BOH and service doors;
- Refuse store doors and locks;
- Plant room and comms room doors;
- Roof access points and hatches;
- CCTV cameras and recording systems;
- External lighting;
- Door closers, locks and ironmongery;
- Signage and wayfinding;
- Any recessed or vulnerable external areas.
- Any damage to doors, glazing, lighting, CCTV, access control equipment, gates, fencing or refuse storage should be repaired promptly.

Why this is important:

Poor maintenance can quickly undermine otherwise effective security measures. A well-maintained hotel communicates ownership, control and active management.

7.17 Summary

The proposed development has a strong basis for a secure city-centre hotel environment, including a defined guest entrance, back-of-house areas, lift/stair cores, refuse provision, plant areas, commercial/tenant interfaces and controlled boundary/gate arrangements.

The security strategy for the site should be based on:

- Controlled access to the hotel entrance, lifts and guest floors;
- Clear separation between public, guest, tenant and staff-only areas;
- Secure management of BOH entrances, goods/service access and refuse areas;
- Protection of basement, plant, substation, comms and roof-level technical areas;
- Secure door, glazing and access control specifications;
- CCTV coverage of key entrances, lift lobbies, BOH areas and vulnerable external interfaces;
- Lighting designed to support safety, surveillance and CCTV performance;
- Management of recessed or less active external areas;
- Clear operational procedures for guests, staff, contractors, deliveries, and refuse collection.

Subject to the implementation of the above recommendations, the development is considered capable of delivering a safe, secure and well-managed hotel environment, consistent with Secured by Design and CPTED principles.

8 Security Recommendation - Quick Checklist:

Notes for Use:

Requirement Type: Distinguishes between mandatory (🟥) and advisory (🟦) measures to assist with prioritisation and implementation.

Standard/Specification: Lists the relevant standards, guidance or best practices applicable to each security feature.

Key Points: Provides a concise summary of the requirement and its intended purpose within the overall security and operational strategy.

This table format allows for quick reference to the recommended measures, associated standards and key actions, supporting the design team, client and stakeholders in implementing a coordinated and proportionate security strategy across the development.

Security Feature	Requirement Type	Standard / Specification	Key Points
Guest Entrance / Hotel Arrival Point	🟥 Mandatory	SBD / CPTED	The guest entrance should be clearly identifiable, well-lit, overlooked where practicable, and covered by CCTV. Entrance management should prevent unauthorised movement from public areas into guest-only or staff-only areas.
Reception / Front-of-House Control	🟥 Mandatory	SBD / Operational Security	Reception/front-of-house areas should support guest management, visitor control, staff oversight and late-night access control. Public access beyond reception should be restricted where required.
Lift Lobby / Guest Floor Access	🟥 Mandatory	SBD / CPTED / Access Control	Lift and lobby arrangements should be controlled so that members of the public cannot freely access guest accommodation floors, staff-only areas, plant rooms or roof-level spaces.
Stair Core Security	🟥 Mandatory	SBD / Fire Strategy Coordination	Stair cores should not provide uncontrolled access from public or lower-level areas to guest floors or restricted areas. Security measures must be coordinated with fire escape requirements.
Emergency Exit Doors	🟥 Mandatory	BS EN 179 / BS EN 1125 / SBD	Emergency exit doors should allow safe escape but prevent unauthorised re-entry. Doors should be self-closing, secure, and monitored or alarmed where appropriate.
Goods Lift / Service Lift Access	🟥 Mandatory	SBD / Access Control	Goods lifts and service lifts should be restricted to authorised staff, contractors or servicing personnel. They should not provide uncontrolled access to guest floors, BOH spaces, basement plant areas or roof/plant levels.

Hotel / Tenant Separation	🟥 Mandatory	SBD / CPTED	Clear separation should be maintained between hotel areas, existing/proposed commercial tenant areas, guest accommodation, BOH spaces and plant/service areas.
Commercial Unit / Tenant Interfaces	🟥 Mandatory	SBD / CPTED	Tenant areas should have clearly defined access arrangements and should not allow uncontrolled movement into hotel guest, staff or back-of-house areas.
Back-of-House Entrance	🟥 Mandatory	SBD / Access Control	BOH entrances should be access-controlled, self-closing, well-lit and covered by CCTV where practicable. Staff-only/service access should be clearly separated from guest/public routes.
BOH Areas and Staff-Only Spaces	🟥 Mandatory	SBD / Operational Security	Back-of-house areas should be restricted to authorised staff and contractors only, with clear access control and staff procedures to prevent tailgating or unauthorised entry.
Refuse Store	🟥 Mandatory	SBD / Best Practice	The refuse store should be secure, lockable, well-managed and well-lit. It should not provide an uncontrolled route into BOH or hotel areas.
Refuse Store Fire / Misuse Risk	🟥 Mandatory	SBD / Best Practice	Refuse storage should be managed to reduce arson, concealment and misuse risks. Waste should be contained and the store kept secured when not in active use.
Basement Plant Areas	🟥 Mandatory	SBD / Operational Security	Basement plant, AHU, switchroom, sprinkler tank, CWS tank, substation and associated technical spaces should be restricted to authorised personnel only.
Comms / IT / Electrical Rooms	🟥 Mandatory	SBD / Operational Security	Comms, IT and electrical rooms should be lockable, access-controlled where appropriate, and separated from guest/public circulation.

Risers and Service Cupboards	🟥 Mandatory	SBD / Operational Security	Mechanical, electrical and essential service risers should be secured to prevent tampering, theft, damage or unauthorised access.
Roof / 8th Floor Plant Access	🟥 Mandatory	SBD / Operational Security	Roof-level and 8th floor plant areas, including access hatches, AHUs, ASHP compound, PV zone, smoke fans and AOVs, should be restricted to authorised staff and contractors only.
External Doors to Restricted Areas	🟥 Mandatory	LPS 1175 SR2 / STS 202 BR2 / LPS 2081 SR B / BS EN 1627 RC3 / PAS 24:2022	External BOH, service, plant and restricted-area doors should meet recognised security standards appropriate to their location and risk.
Guest / Public Entrance Doors	🟥 Mandatory	PAS 24:2022 / SBD / Manufacturer Security Specification	Public-facing entrance doors should be robust, secure and compatible with access control, fire strategy and operational management requirements.
Accessible Windows and Glazing	🟥 Mandatory	BS EN 356 P1A minimum where appropriate	Accessible or vulnerable glazing at ground/lower levels or public-facing elevations should include laminated glazing or equivalent protection appropriate to risk.
CCTV Coverage	🟥 Mandatory	BS EN 62676 / NSI or SSAIB installer preferred	CCTV should cover the guest entrance, reception/front-of-house area, BOH entrance, refuse store access, lift lobby areas where appropriate, plant/service access points and vulnerable external interfaces.
CCTV Data and Signage	🟥 Mandatory	UK GDPR / Data Protection Act / ICO Guidance	CCTV signage and data handling procedures should comply with relevant data protection requirements.

External Lighting	🟥 Mandatory	BS 5489:2020	Lighting should cover guest entrances, BOH entrances, refuse access, service points, escape doors, external frontages and any recessed or less active areas.
Lighting Note	🟥 Mandatory	SBD / Best Practice	Decorative or low-level lighting alone should not be relied upon for security-critical areas such as entrances, BOH access, refuse areas, service doors and plant access points.
Recessed / Less Active Areas	🟥 Mandatory	SBD / CPTED	Recessed areas, corners, service doors, escape doors and less active external edges should be well-lit, visible and managed to reduce loitering, concealment and misuse.
Proposed Gates / Fence Interface	🟥 Mandatory	SBD / CPTED	Where the proposed gates/fence are shown, these should be robust, lockable and managed to prevent unauthorised access to BOH/refuse or restricted service areas.
Guest Room Floors	🟥 Mandatory	SBD / Access Control	Guest accommodation floors should operate as controlled zones, with access managed through lift/stair controls, staff procedures and secure separation from public/tenant areas.
Housekeeping Areas	🟥 Mandatory	SBD / Operational Security	Housekeeping rooms/stores should be lockable and restricted to authorised staff only, particularly where cleaning materials, linen, equipment or service access is provided.
Signage and Wayfinding	🟦 Advisory	SBD / CPTED	Signage should clearly distinguish hotel entrance, tenant areas, staff-only zones, BOH areas, emergency exits and restricted plant/service areas.

Hotel Management Procedures	🟥 Mandatory	Operational Security / Best Practice	Procedures should cover guest access, visitor management, staff access, key/fob/card management, contractor control, deliveries, refuse collection, CCTV review, incident reporting and late-night entrance management.
Maintenance Strategy	🟦 Advisory	Best Practice	Maintain doors, locks, access control, CCTV, lighting, refuse-store security, signage, gates/fencing, plant access points and any vulnerable external areas to preserve security performance.
Designing Out Crime Officer Review	🟦 Advisory	SBD / Local Police Consultation	If required by the Local Authority or Police, the final detailed security design should be reviewed with the relevant Designing Out Crime Officer.

9 Conclusion

It is concluded that the proposed redevelopment of Maybrook House, 40 Blackfriars Street, Manchester, M3 2EG, is capable of delivering a safe, secure and well-managed hotel environment, subject to the implementation of the recommendations outlined within this report.

The proposed security strategy is proportionate to the identified risks and is based on a combination of controlled access, clear separation between public, guest, tenant and back-of-house areas, appropriate physical security measures, CCTV coverage, external lighting, and clear operational management procedures, in line with the principles of Secured by Design (SBD) and Crime Prevention Through Environmental Design (CPTED).

This conclusion is based on an assessment of the proposed layout, access arrangements, hotel guest areas, commercial/tenant interfaces, lift and stair cores, back-of-house areas, refuse store, basement plant areas, comms/electrical spaces, roof-level plant access and the wider city-centre context surrounding the site. Particular consideration has been given to the relationship between the public realm and the proposed hotel use, including the management of guest access, staff/service access, refuse arrangements, plant access and the separation of hotel areas from existing or proposed commercial tenant spaces.

Subject to the implementation of the recommendations, no significant safety or security concerns have been identified that would preclude the development from achieving a secure and well-managed hotel environment or progressing through planning.

This report supports the design team in aligning the scheme with Secured by Design principles, CPTED guidance and the Local Authority's requirement for a proportionate Crime Impact Statement / Security and Operational Strategy. Final confirmation of any Secured by Design compliance or award remains subject to review and approval by the relevant Designing Out Crime Officer, where applicable.

This assessment has been prepared based on the information available at the time of writing, including drawings, supporting documentation, available crime data and a desk-based appraisal. Should the design, layout, use, tenant arrangements or operational strategy change, this assessment should be reviewed and updated accordingly to ensure continued alignment with relevant guidance and best practice.



10 Appendix A

10.1 Evidencing Security Needs: Crime Statistics and Trends

This section provides a focused visual analysis of the available crime information relevant to the development, including Police.uk/data.police.uk material where available, noting the known limitations in current Greater Manchester Police data provision. The information is supplemented by broader Manchester crime comparison data and GMP-published neighbourhood crime information where available.

These visuals support the security recommendations and provide useful context for understanding the local crime landscape, while recognising the data limitations noted within this report. Stakeholders will gain a clear insight into the area's crime landscape, which is crucial for crafting effective security strategies.

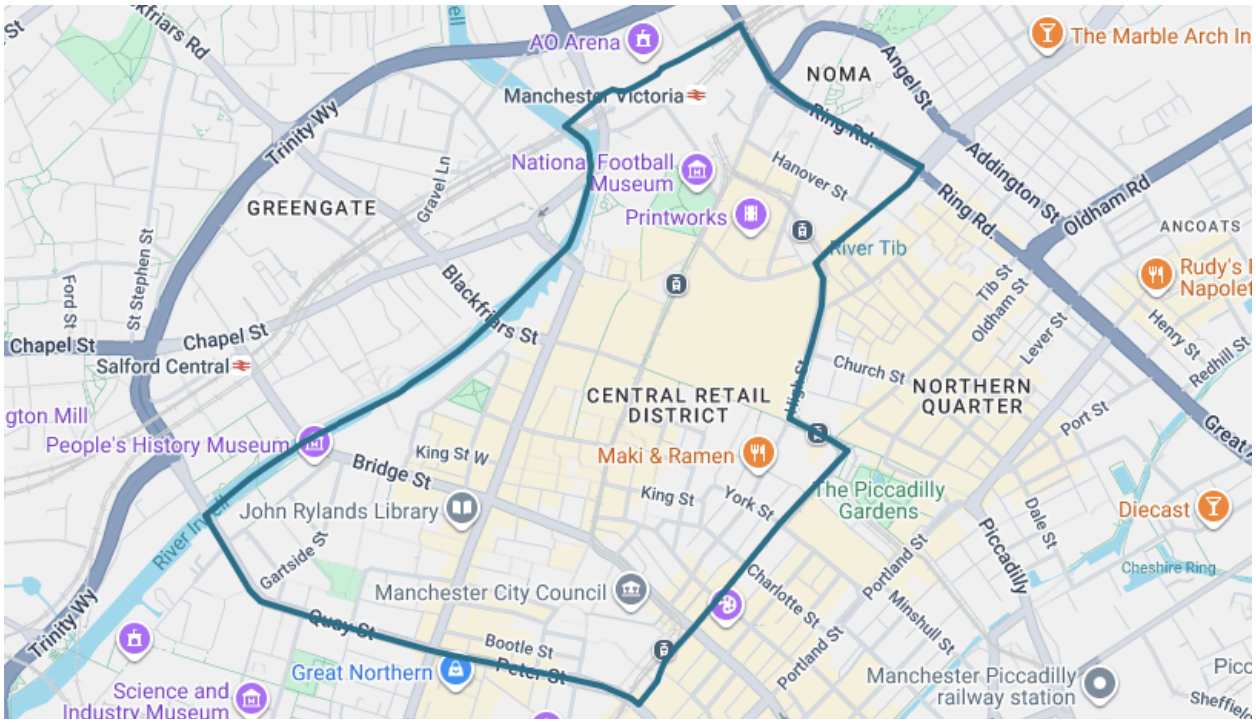


Figure 03 - Commercial District 'Policing Neighbourhood' (Source: Police.uk)

11 Appendix B

11.1 Further crime statistics

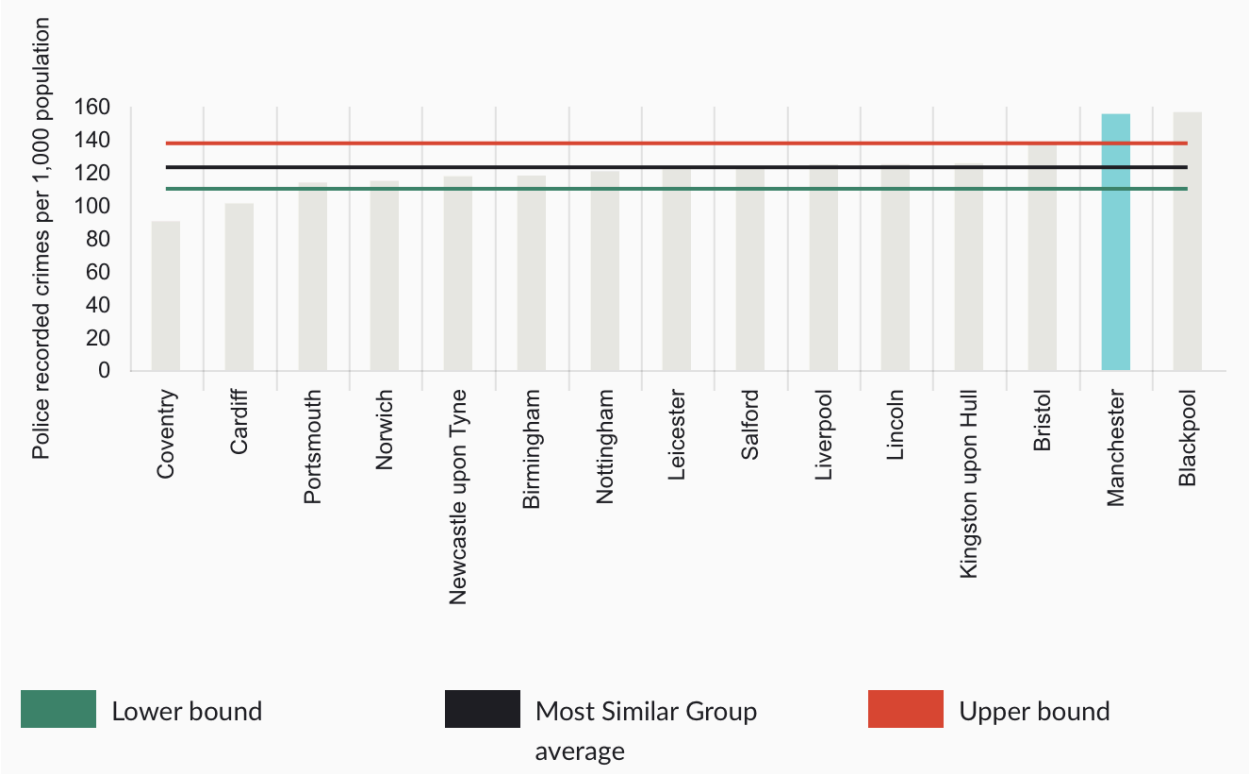


Figure 04 - Crime in Manchester compared with crime in similar areas (ending in Sep 2025).

In the year ending September 2025, the crime rate in Manchester was higher than the average crime rate across similar areas.

The red and green lines show how far the crime rate would normally vary from the average. Manchester lies above the red line, so its crime rate is higher for the group.

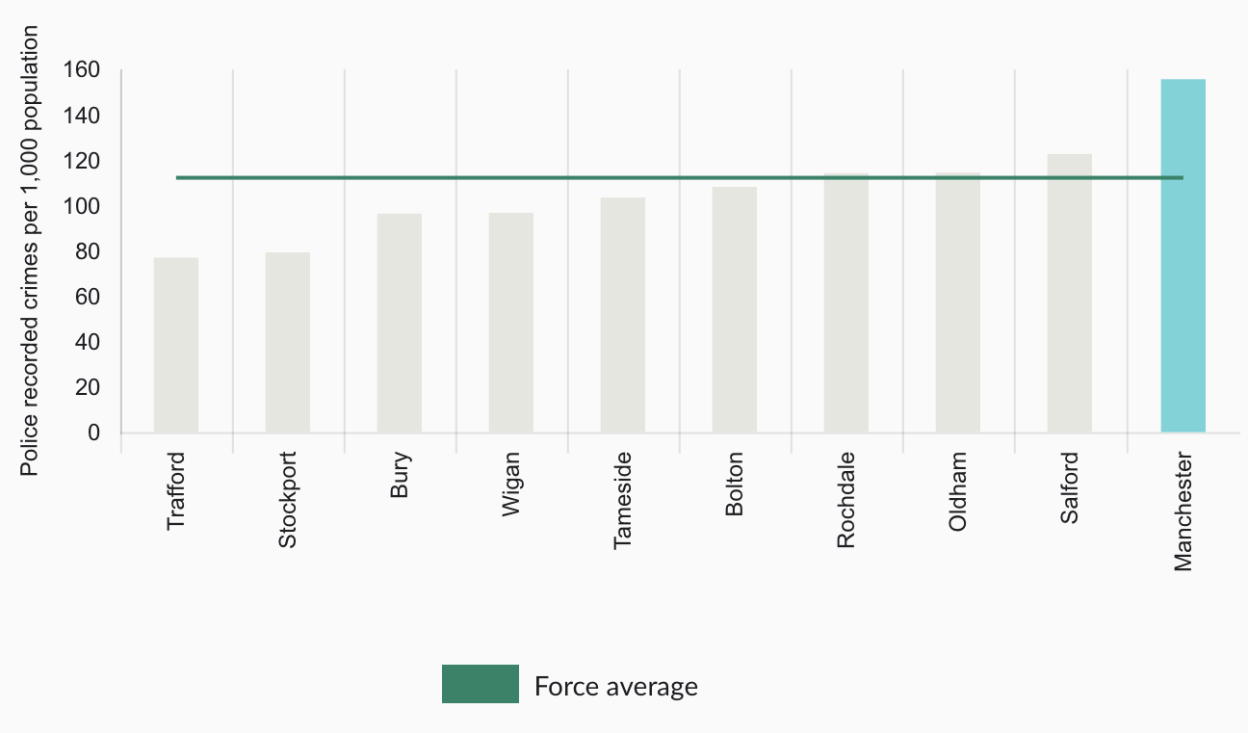


Figure 05 - Crime Stats of the Manchester area compared to Greater Manchester Force Area (ending in Sep 2025).

In the year ending September 2025, the crime rate in Manchester was higher than average for the Greater Manchester area.

This chart compares the crime rate in your local area to the average crime rate across the force area. It shows the total number of crimes over twelve months per thousand residents, for the crime type selected.

In the quarter ending September 2025, the crime rates were:

- up in Manchester
- down in the Greater Manchester force area

compared with the corresponding quarter in 2024.

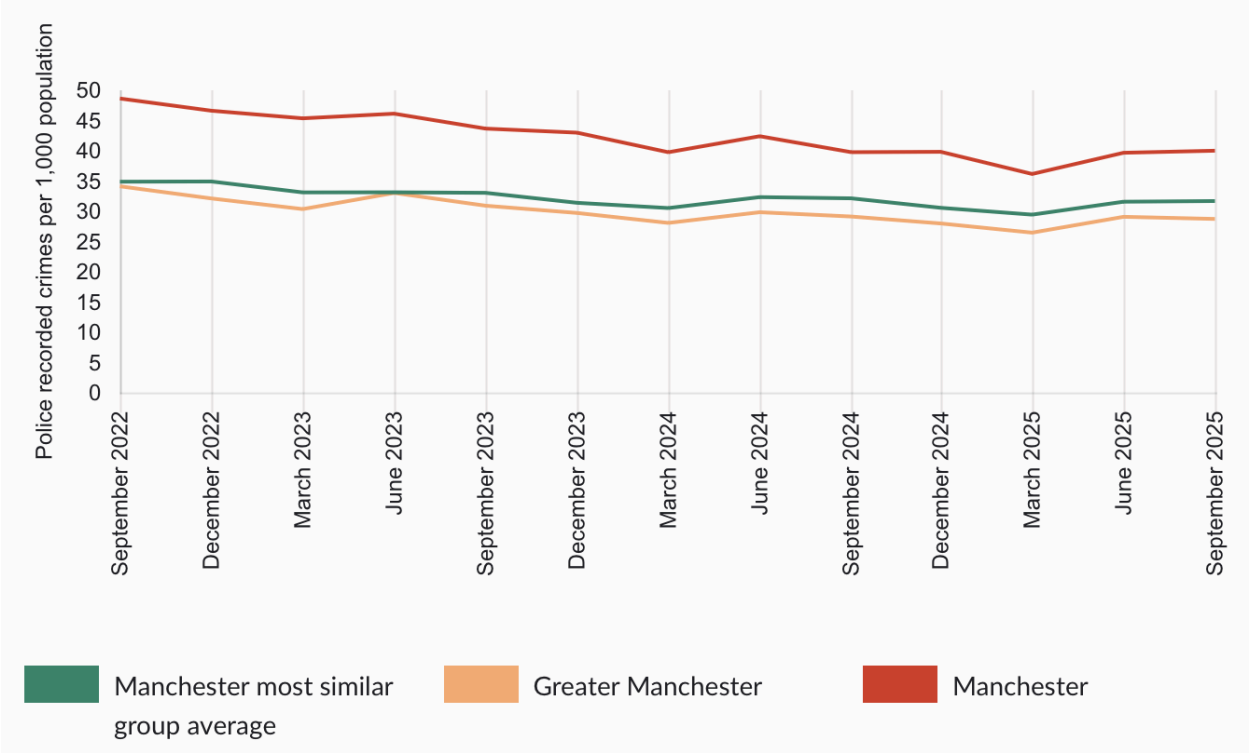


Figure 06 - Crime changes over time in Manchester and the Greater Manchester force area.

This chart shows how crime rates in your local area and the police force area have changed over time. It also shows how the average crime rates in similar areas to your local area have changed over time.

12 Appendix C

12.1 Architectural Plan Review: A Security Perspective

Proposed Lower Ground Floor

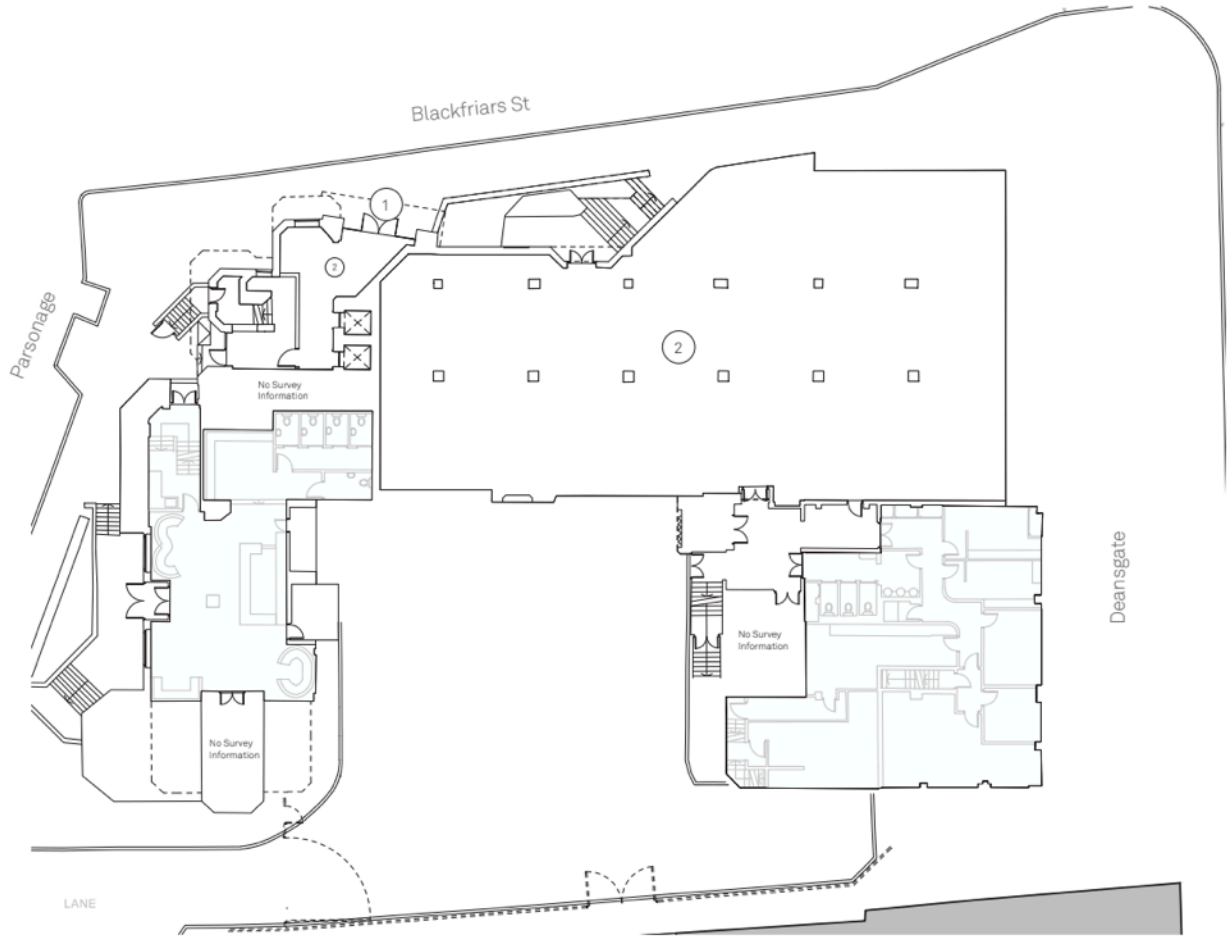


Figure 07 - Proposed Lower Ground Floor - (Source: JMA)

Proposed Ground Floor Plan

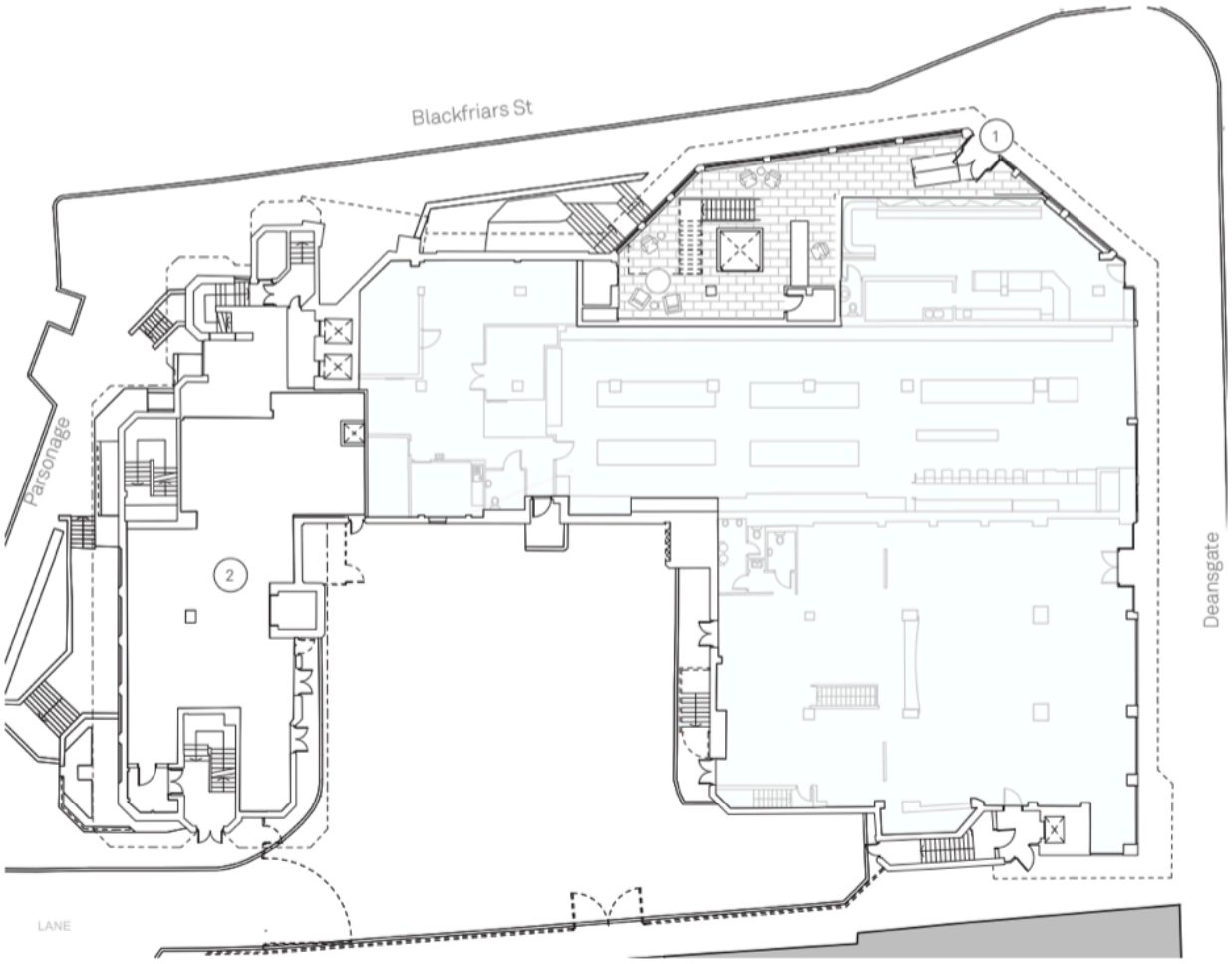


Figure 08 - Proposed Ground Floor Plan - (Source: JMA)

Proposed First Floor Plan

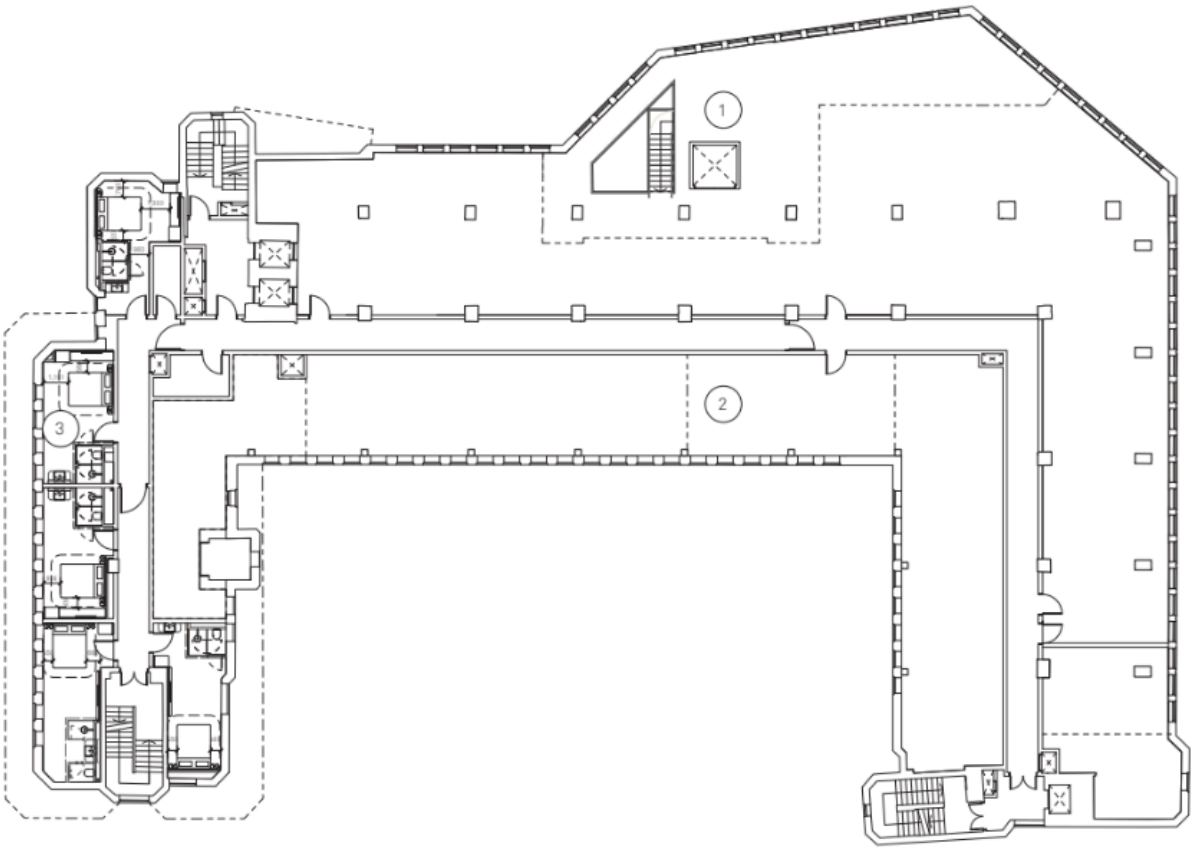


Figure 09 - Proposed First Floor Plan - (Source: JMA)

Proposed Second to Fifth Floor Plan

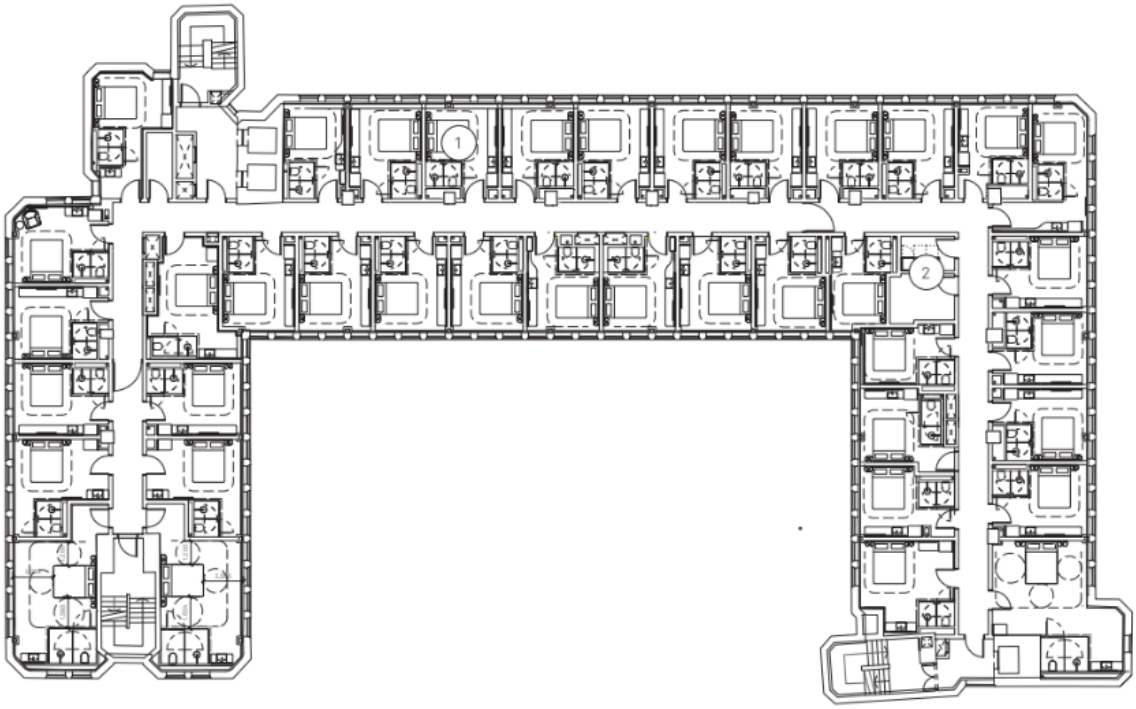


Figure 10 - Proposed Second to Fifth Floor Plan - (Source: JMA)

Proposed Sixth to Seventh Floor Plan

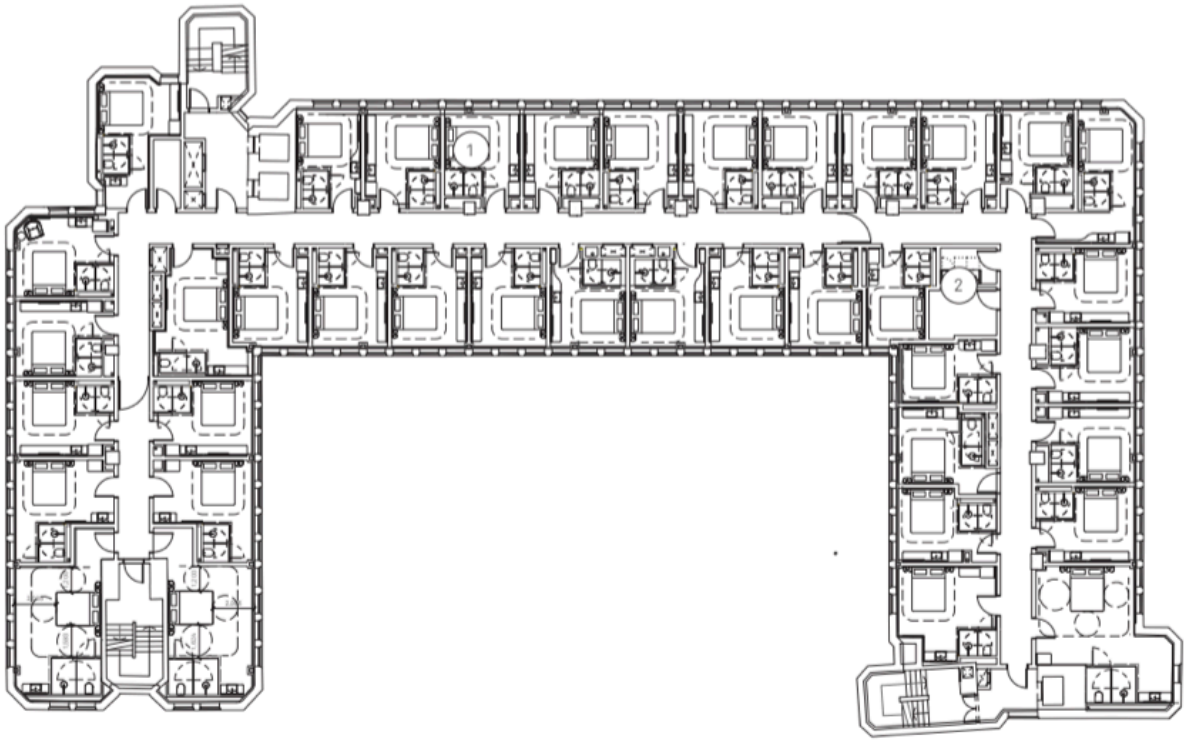


Figure 11 - Proposed Sixth to Seventh Floor Plan - (Source: JMA)

13 Appendix D

13.1 SQSS Credentials

Suitably Qualified Security Specialist (SQSS) Statement

This report has been prepared by Nasr Haque MSyI, Director and Security Consultant at Graphite Security Ltd.

Nasr Haque is an experienced security consultant with approximately 10 years of experience within the crime prevention, security design and built environment security field. He holds Member-level membership of The Security Institute (MSyI) and has completed Secured by Design training through the College of Policing. Nasr Haque also holds a full Secured by Design licence, enabling him to provide specialist advice and reporting aligned with Secured by Design principles and guidance. His work includes the preparation of Crime Impact Statements, Security Needs Assessments, Secured by Design reviews, BREEAM Hea06 security assessments, CPTED-based design reviews, and security recommendations for planning submissions.

For the purposes of this assessment, the SQSS role has included, where relevant:

- Review of the proposed architectural drawings, site layout and supporting information;
- Review of the site context and available local crime profile;
- Identification of project-specific crime and security risks;
- Assessment of access, movement, public/private interfaces, operational areas, external spaces and relevant security-sensitive locations;
- Consideration of physical security, access control, CCTV, lighting, management and operational security requirements;
- Preparation of proportionate security recommendations aligned with SBD, CPTED and relevant good practice principles;
- Integration of security and operational considerations to support a safe, secure and well-managed development.

The recommendations contained within this report are based on the information available at the time of writing and are intended to support the planning/design process by demonstrating that crime prevention and security have been considered in a proportionate and design-led manner.

13.2 Professional Background

Credential / Experience	Details
Name	Nasr Haque MSyI
Position	Director / Security Consultant
Company	Graphite Security Ltd
Professional Membership	Member-level membership of The Security Institute (MSyI)
Secured by Design Status	Full Secured by Design licence holder
Training	Secured by Design training completed through the College of Policing
Relevant Experience	Approximately 10 years within crime prevention, security design and built environment security
Project Role	Suitably Qualified Security Specialist / Security Consultant

13.3 Relevant Experience

Nasr Haque has experience across a range of development types, including:

- Commercial and industrial developments;
- Residential and mixed-use developments;
- Hotel, hospitality and public-facing environments;
- Education developments;
- Healthcare projects;
- Retail and town-centre environments;
- BREEAM security assessments;
- Planning-stage security and crime prevention submissions.
- His work regularly includes:
- Crime Impact Statements;
- Security Needs Assessments;
- Secured by Design reviews;
- BREEAM Hea06 security assessments;
- CPTED-based design reviews;
- Physical security recommendations;
- Access control, CCTV, lighting and external security reviews;
- Security strategies for planning submissions.

13.4 Competency Basis

This assessment has been prepared with reference to relevant crime prevention and security design principles, including:

- Secured by Design principles and guidance;
- Crime Prevention Through Environmental Design (CPTED);
- ISO 22341 principles, where relevant;
- Relevant physical security standards referenced within this report;
- Planning-related crime prevention expectations;
- Available local crime data and site context analysis.

The assessment applies a proportionate, risk-based approach, taking into account the nature of the proposed development, its operational requirements, the relevant site context and the identified local crime profile.

13.5 Declaration

I confirm that this report has been prepared using my professional judgement as a security consultant and is based on the information available at the time of writing.

The recommendations provided are proportionate to the identified risks and are intended to support the delivery of a safe, secure and well-managed development.

Prepared by:
Nasr Haque MSyI
Director | Security Consultant
Graphite Security Ltd