Security Needs Assessment

Queen Street, Tottenham

Figure 01 - Proposed Elevation (Source: PRC Architecture)

Document control

Job Title	Queen Street
Job Number	R056
Report Title	Security Needs Assessment
Document No.	R056-GSL-SY-ZZ-RP-Y-0001-S4-A
Date of Issue	15-03-2024
Compiled By	Nasr Haque

Contact

Nasr Haque	nasr.haque@graphite-security.co.uk

Revision control

	Purpose	Date
REV A	Issued for comment.	15-03-2024

GRAPHITE SECURITY

Table of Contents

1 Introduction

This report details the findings of a Security Needs Assessment (SNA) carried out by Graphite Security in support of the planning and construction of the proposed industrial use at Queen St, London N17 8HZ previously known as Booker Tottenham.

The SNA examines security threats to the planned development and identifies security vulnerabilities present in the architectural designs and intended uses. The SNA adheres to a security design methodology to provide security recommendations that should be incorporated into future project stages. These recommendations are specifically aimed at mitigating security risks to the development, its users, and the surrounding area.

Site address:
Queen St,
London.
N17 8HZ.

Figure 02 - Site Location Plan (Source: Google Maps)

1.1 BREEAM Hea 06 Security Credits

The actions conducted, as well as the structure and content of this report, align with the specifications outlined in BREEAM NC V6 Hea 06.

1.2 Security Recommendations

Within this SNA report, various options for mitigating security risks are presented for consideration. These recommendations are intended to address security concerns related to the development practically and proportionately, while also taking into account their potential impact on the proposed budget, functionality, and aesthetics of the building.

We invite comments on the security recommendations contained in this report from both the client and design team, as this input is crucial to ensuring that these recommendations align with the operation, design, and budget of the project.

BREEAM NC V6 Hea 06 Requirements:	How we meet those 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)”	Graphite staff are licensed under both the Secured by Design (SBD) and Security Assurance BRE (SABRE) security accreditation schemes. The SNA requirements were completed in Dec 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 at the time of writing this report. We are yet to hear back.
“Identify risks specific to the proposed, likely or potential use of the building(s)”	Described in the relevant section of this report.
“Identify risks specific to the proposed, likely or potential use of the building(s)”	Described in the relevant section of this report.
“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”	Graphite Security 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.

2 Development & Surroundings

Figure 03 - Proposed Site Plan (Source: Google Maps)

Queen Street in London, N17 8HZ, is located in the culturally rich borough of Haringey, offering a mix of traditional and modern residential options amidst green spaces that provide a serene environment.

The area enjoys excellent connectivity through a comprehensive public transport network, including buses, the London Overground, and Underground services, facilitating easy access to the wider city and its attractions. This combination of tranquil living spaces and convenient transportation options makes Queen Street a desirable location in London.

3.0 Site Survey

Figure 04 - Site Survey (Source: Google Maps)

4 Development Layout & Uses

Figure 05 - Proposed Site Plan (Source: PRC Architecture)

The proposed development comprises three units enclosed by a secure perimeter fence. A single main access point will establish a secure one-way entry and exit system, ensuring safety. Additionally, green spaces will be incorporated into the design.

5 Crime Risk Assessment

Crime data analysis is a crucial component of understanding and addressing the complex issues related to public safety and law enforcement. In this section, we delve into a comprehensive examination of crime statistics and trends, drawing upon data from police.uk and other open sources.

By dissecting the available crime data, we aim to provide valuable insights that can inform the design team aimed at enhancing the safety and well-being of our society.

Based on the information accessible by the police.uk, the crime and disorder in the 'Bruce Castle' policing neighbourhood (which falls under Metropolitan Police) over the past 12 months have been characterised by the following primary categories:

- Anti-social Behaviour
- Violence and Sexual Offences
- Vehicle Crime
- Other Theft

Please refer to Figure 09 for a breakdown of all crime types in the Bruce Castle neighbourhood between Feb 2023 and Feb 2024. Additional information in section 18.1.

Please refer to the Appendix below for the figures mentioned above.

6 Threat Actors:

Potential Extreme Scenario Risk:
Random theft can impact industrial settings, occurring when a thief in a legitimate public area (like a Public Pathway or Parking) notices a security weakness. Reports, including police records, commonly note that most random thefts involving entry happen through doors left open, unlocked, or unmonitored.

Typically, the skill level of random thieves is low, as they avoid carrying tools that might be classified as 'prepared for burglary'. A lone individual aims to enter the building through open or unsecured doors or windows, usually beginners without tools.

Discreet. Risk:
Fraudulent Entry Like random theft, fraudulent entry involves trickery to gain access to premises and is often viewed as a lower-risk strategy by criminals. Frequent tactics include posing as utility workers or authorities to gain staff trust and access to a building, or various uses to persuade staff to open a door, potentially leading to forced entry. An individual attempts to enter the building by impersonating a service engineer or authority figure to gain staff trust and access.

Not identified as overtly aggressive or discreet. Risk:
Deliberate Theft of industrial units is sometimes targeted by professional criminals for breaking and entering if they are thought to house valuable items like cash, jewellery, electronics, mobile phones, apparel, and office supplies. Several individuals try to enter the building and bypass security using a variety of hand tools. Openly aggressive.Informed attackers, employing small hand tools and electronic gadgets.

7 Security Design Methodology - Design Basis Threat (DBT)

The Design Basis Threat (DBT) refers to a profile of an adversary's type, composition, and capabilities. It is used in security and risk management, especially in the context of critical infrastructure protection, nuclear facilities, and high-value assets. The DBT helps in understanding the potential threats and their characteristics, such as the tactics, weapons, and resources the adversary might use, and their level of motivation and expertise.

Capabilities: The skills and resources the adversary possesses. This can include technical know-how, access to weapons, and the ability to recruit insiders.

Intent: The adversary's objectives and motivation. This aspect delves into why the adversary might target the facility or asset, whether for political, ideological, financial, or personal reasons.

History and Precedence: Past incidents and attempts, either at the same location or similar facilities, provide insight into possible threat scenarios.

Innovation and Tactics: The ability of the adversary to adapt and employ new methods or technologies to overcome security measures.

The DBT is not static; it evolves with changes in the security landscape, technological advancements, and shifts in geopolitical situations. It is a crucial part of a layered security strategy, guiding the design of physical, technological, and procedural security measures to mitigate identified risks. The goal is to ensure that security measures are proportionate to the threat and capable of effectively countering it.

7.1 Site-specific DBTs

Attack Category	Description
Opportunistic Theft: Non-Forceful Entry Without Violence	One threat actor endeavours to achieve unauthorised access to the building without resorting to force or violence. The intruder will refrain from carrying conspicuous tools or employing noisy techniques
Targeted Theft: Skilled Intrusion Involving the Use of Tools and/or Violence.	Two proficient intruders, armed with covert hand tools, are attempting to gain entry into the building. These attackers are willing to generate noise if required, for instance, by forcibly entering through a rear door to access the building.

8 Layers of Physical Security: A Comprehensive Approach to Protection

Perimeter Security: This is the outermost layer and involves measures to secure the physical boundaries of a facility. It can include features like fences, walls, gates, access control points, and barriers to prevent unauthorised entry.

Access Control: Access control is a critical layer that regulates who can enter and exit a facility. It includes measures like card readers, keypads, biometric scanners, and security personnel who monitor and control access to buildings or specific areas within a facility.

Security Surveillance: Security cameras and monitoring systems provide continuous surveillance, recording activities, and providing a deterrence factor. They can also be used for investigations in case of incidents.

Intrusion Detection Systems (IDS): IDS systems are designed to detect unauthorised entry or security breaches. They include sensors, alarms, and notifications to alert security personnel when there's a breach.

Security Lighting: Adequate lighting is essential for deterring criminals and enhancing visibility. Well-lit areas are less likely to be targeted for criminal activity.

Physical Barriers: These are additional layers within a facility, such as secure doors, reinforced windows, safes, and locks, designed to protect specific assets or areas.

Security Personnel: Trained security personnel, such as guards or receptionists, provide a human presence to monitor access, respond to incidents, and enforce security policies.

Security Policies and Procedures: Effective security also relies on well-defined policies and procedures that govern how security measures are implemented and enforced. This includes protocols for handling incidents, access control, and emergency response.

Emergency Preparedness: Having plans and resources in place for emergency situations, such as fires, natural disasters, or security breaches, is crucial. This includes evacuation plans, fire suppression systems, and emergency communication systems.

Physical Redundancy: In some cases, redundancy in critical systems and assets can be considered a layer of physical security. This involves having backups or duplicates of essential equipment or systems to ensure continuity in case of failures.

Visitor Management: Properly managing and monitoring visitors to a facility is essential. This can include sign-in procedures, visitor badges, and escort requirements for visitors in secure areas.
Employee Training: Ensuring that employees are trained in security awareness and know how to follow security protocols is a fundamental layer of physical security.

Each of these layers contributes to the overall security of a facility, and organisations typically assess their specific needs and risks to determine which layers are most appropriate for their situation. Additionally, a layered approach to physical security is often more effective than relying on a single security measure, as it provides multiple lines of defence against potential threats.

9 Security Requirement Statements

9.1 Queen Street - Security Requirements Statement

The security requirements for the Queen Street development encompass the following objectives:

- Create security features that enhance the marketing and operation of the development by meeting or surpassing the expectations of potential guests.
- Establish a visible and reassuring security presence without appearing overly imposing.
- Foster a safe and secure environment for staff, guests, and assets, minimising security risks to a level deemed reasonably practicable, considering "reasonable worst-case" security threats.
- Manage the environment as a controlled space, permitting access beyond semi-public areas only to authorised individuals.
- Implement a resilient building envelope that deters and delays potential threat actors from entering the site, harming occupants, or removing property.
- Address the Design Basis Threat, encompassing:
    - Opportunistic entry and theft.
    - Experienced forced entry employing manual attack techniques.

10 Security Management and Control

A dedicated location should be provided on-site to allow the building management team to manage the site and building access, monitor the site's video surveillance and intruder alarms and coordinate an emergency response.

10.1 Recommendations:

- Provide a security monitoring and control location within the building. This need not be a dedicated Security Control Room, a suitably located and equipped building management room may suffice.

- Provide security monitoring and control location with an intercom connected to the building entrances.

- Provide the security monitoring and control location with head-end equipment for access control, intercom, intruder alarms and video surveillance.

11 Crime Prevention Through Environmental Design

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

11.1 Recommendations:

- Provide suitable illumination to accessible areas around the buildings, including public open areas, all pedestrian routes, and service roads.
- Provide suitable illumination to service areas in and around the buildings.
- Provide detector-activated lighting to recesses and doorways.
- Provide clear demarcation of the extent of semi-public areas in the buildings, e.g. transitions from reception areas or lobbies (semi-public) to circulation (semi-private) or back of house (private). Consider using signage and changes in colour and materials.
- Provide security signage at entrance points.
- Consider signage describing video surveillance (required by legislation) and security patrols.

12 Recommendation – Physical Security

12.1 Recommendations - Boundary Treatment:

- Provide a boundary treatment to the site with a minimum height of 1.8m. We would recommend welded wire mesh fencing securing the units and car park with access-controlled vehicle entrances.

12.2 Recommendations - External Doors:

- Provide back-of-house external doors, e.g. the delivery and dispatch area and fire exits, with doorsets certified to LPS 1175 (noisy manual attacks) Security Rating 2 or LPS 2081 (stealth attacks) Security Rating B.

- Consider providing comms, IT, critical plant, valuable storage and security spaces with entrance doorsets certified to LPS 1175 SR1.

12.3 Recommendations - Glazing:

- Provide laminated glass to accessible glazed areas. (ground floor only). If compatible with the selected glazing system, use glass rated P1A or above under BS EN 356. If this is not possible, glazing should incorporate a PVB interlayer of a minimum thickness of 0.76 mm.

13 Recommendation – Intruder Alarm

To assist the local police and possible onsite security team in responding to security incidents we recommend that an intruder and duress alarm system be 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.

13.1 Recommendations:

- Provide an intruder alarm system to landlord Areas.

- **Consider** providing magnetic door contacts to doors from landlord areas to external areas and to accessible opening windows in landlord areas.

- **Consider** providing volumetric detectors in landlord areas with accessible glazing or external doors (other than those that will be permanently occupied).

14 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.

14.1 Recommendations:

- Provide access control and intercom to all main entrances allowing staff and guests access to the building.
- Provide access control to all staff-only entrances.
- Provide access control to doors into back-of-house areas, e.g. Refuse and Bicycle Store.
- Provide access control to doors into stairs from the ground floor.
- Provide access control to doors from semi-public front-of-house areas into back-of-house circulation and spaces e.g. Cycle Store and Refuse.
- Provide access control to doors from back of house spaces e.g. Refuse and Cycle Storage into circulation and common areas.

15 Video Surveillance

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.

16 External Video Surveillance

16.1 Recommendations:

- Provide fixed external cameras viewing all entrances.
- Provide fixed external cameras viewing the pedestrian access routes to the site via external amenity spaces.

17 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 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

18 Appendix

18.1 Crime Data:

Policing Neighbourhood: 'Bruce Castle'

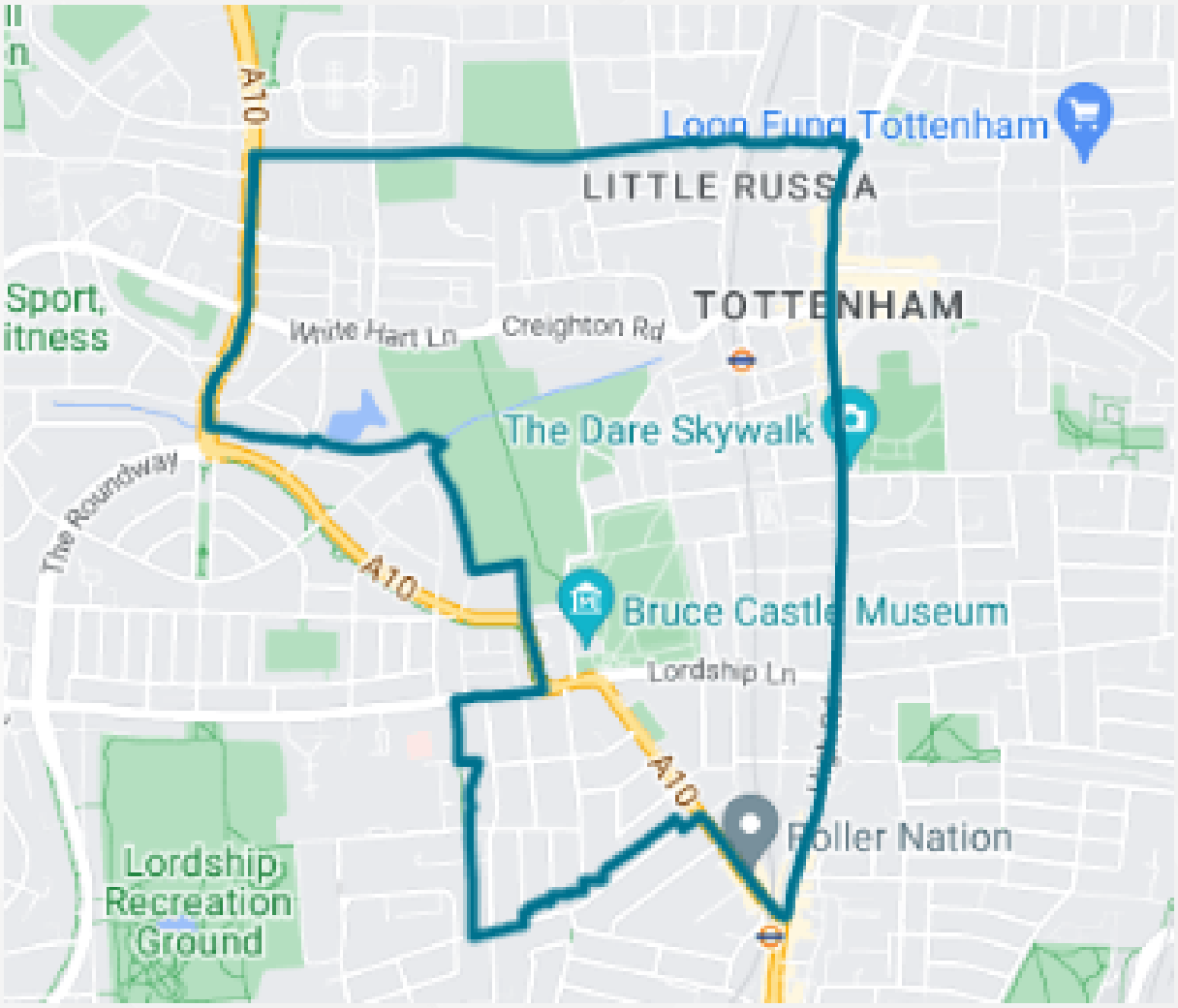

Figure 06 - Area Boundary (Source: Police. uk)

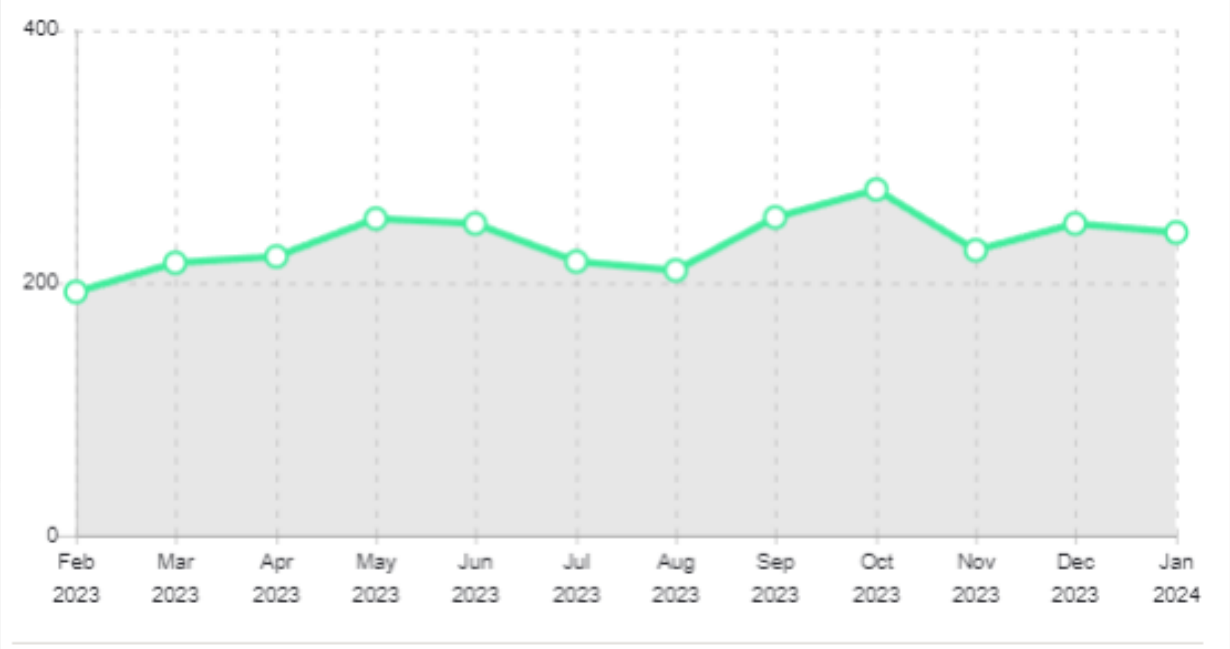

Figure 07 - Crime Levels Overview Feb 23 - Jan 24 (Source: Police. uk)

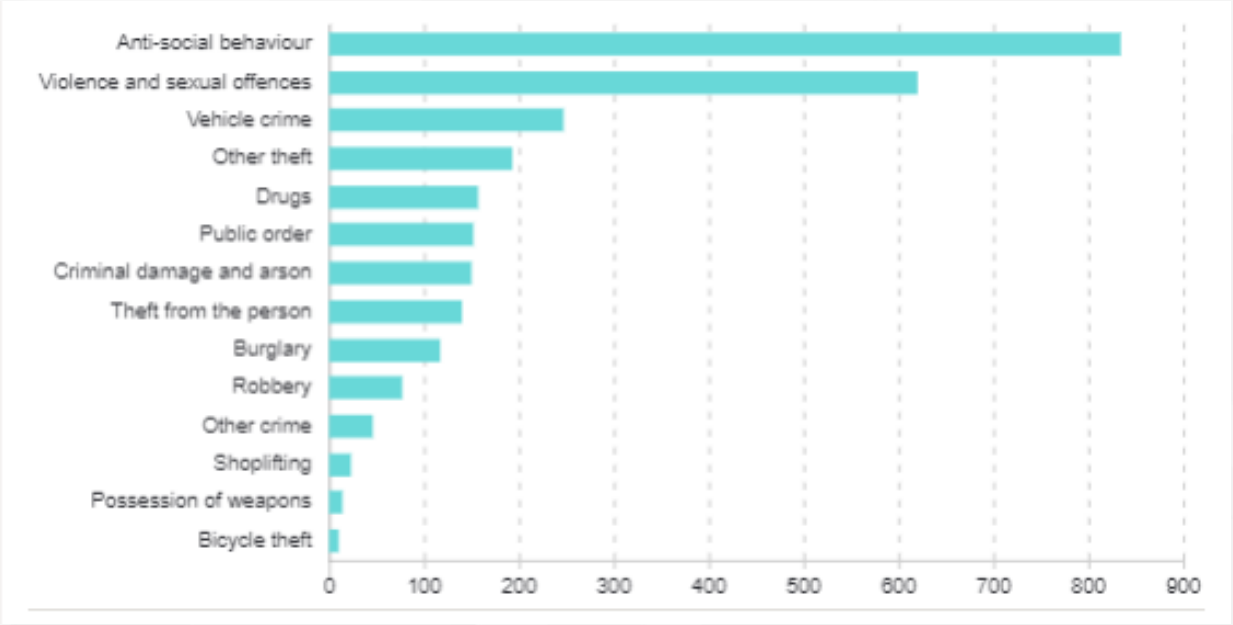

Figure 08 - Crime Types Overview Feb 23 - Jan 24 (Source: Police. uk)

18.2 Neighbourhood Picture

The following table and graphs show you crime and ASB breakdowns and trends for Bruce Castle.

	ASB	Burglary	Robbery	Vehicle	Violent	Shoplifting	CD&A	Other Theft	Drugs	Bike Theft	Theft From the Person	Weapons	Public Order	Other	Total
Jan 2024	55	21	4	16	56	0	22	17	17	0	13	2	12	1	236
Dec 2023	69	5	8	17	41	0	23	20	22	3	18	0	16	1	243
Nov 2023	77	13	4	28	40	2	13	10	10	3	13	0	7	2	222
Oct 2023	91	6	7	19	67	4	16	12	15	1	11	3	14	4	270
Sep 2023	76	9	4	27	53	1	17	14	15	0	12	2	17	2	249
Aug 2023	82	8	3	9	45	6	6	12	12	2	5	1	10	8	209
Jul 2023	61	14	7	23	58	1	7	13	7	0	7	1	12	5	216
Jun 2023	65	9	10	28	56	0	11	27	11	0	17	0	6	4	244
May 2023	83	5	10	14	64	1	9	19	14	0	16	2	9	3	249
Apr 2023	70	8	3	26	40	3	5	22	16	0	7	0	18	2	220
Mar 2023	66	12	3	20	47	4	11	11	5	0	12	4	12	6	213
Feb 2023	40	8	14	21	42	2	10	12	14	2	7	0	11	9	192

Figure 09 - All crime types in Newton between Feb 2023 to Jan 2024.

The crime rate peaked in Oct 2023 dominated by violence and anti-social behaviour. The lowest recorded crime recorded was in Feb 2023 dominated by violence and anti-social behaviour.

18.3 Compare your area

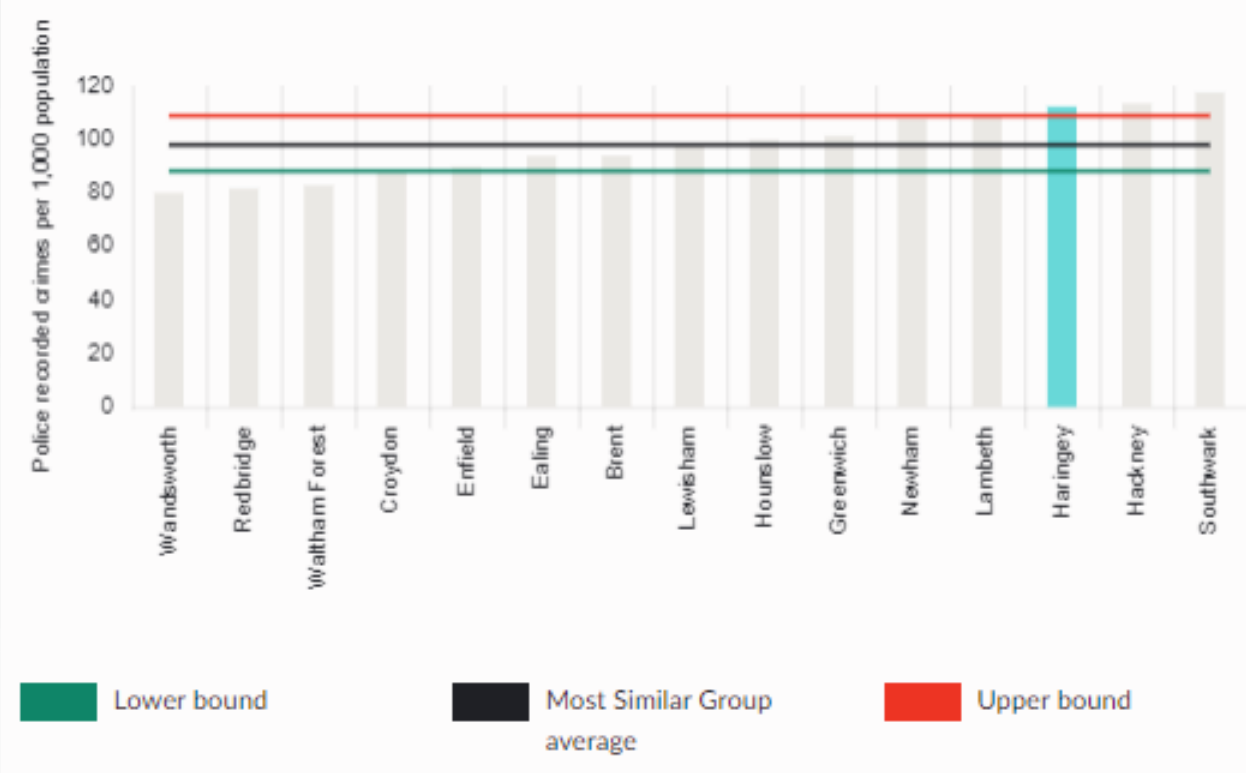

Figure 10 - Crime in Haringey compared with crime in similar areas (ending in Sep 2023).

This chart compares the crime rate in your local area to the average crime rate across similar areas. It shows the total number of crimes over twelve months per thousand residents, for the crime type selected. The red and green lines show how far the crime rate would normally vary from the average. Hatingey lies above the red line, so its crime rate is above the upper-bound group.

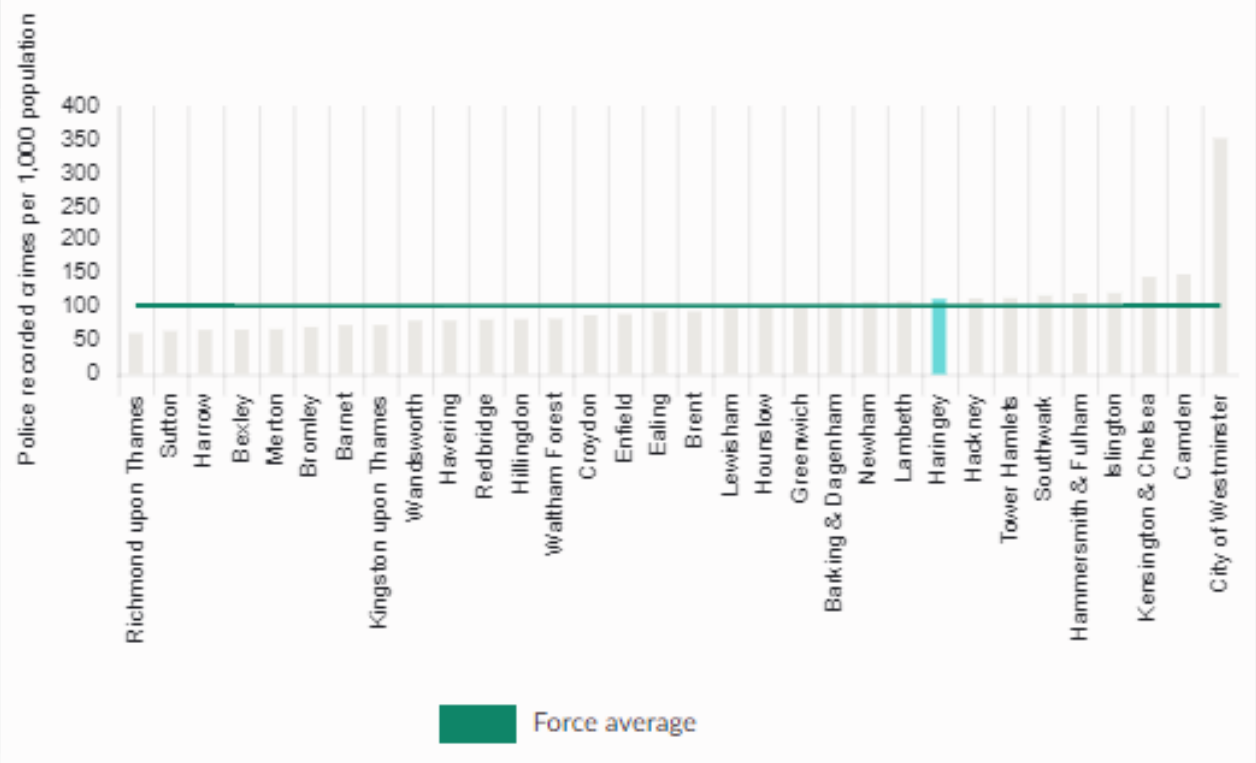

Figure 11 - Crime Stats of Haringey area compared to Metropolitain Force Area (ending Sep 2023).

The force's average crime rate is 101.95 and the Haringey area is 112.14 showing it is above the Metropolitain force average.

The above figure shows all areas within the Metropolitan Force Area comparing it to the force's average crime rate, as you can see Haringey, where the development is situated is located on the higher end of the chart, with Haringey being the 9th highest rated area.

In the quarter ending Sep 2023, crime rates were:

- up in Haringey
- up in the Metropolitan Force area

compared with the corresponding quarter in 2022.

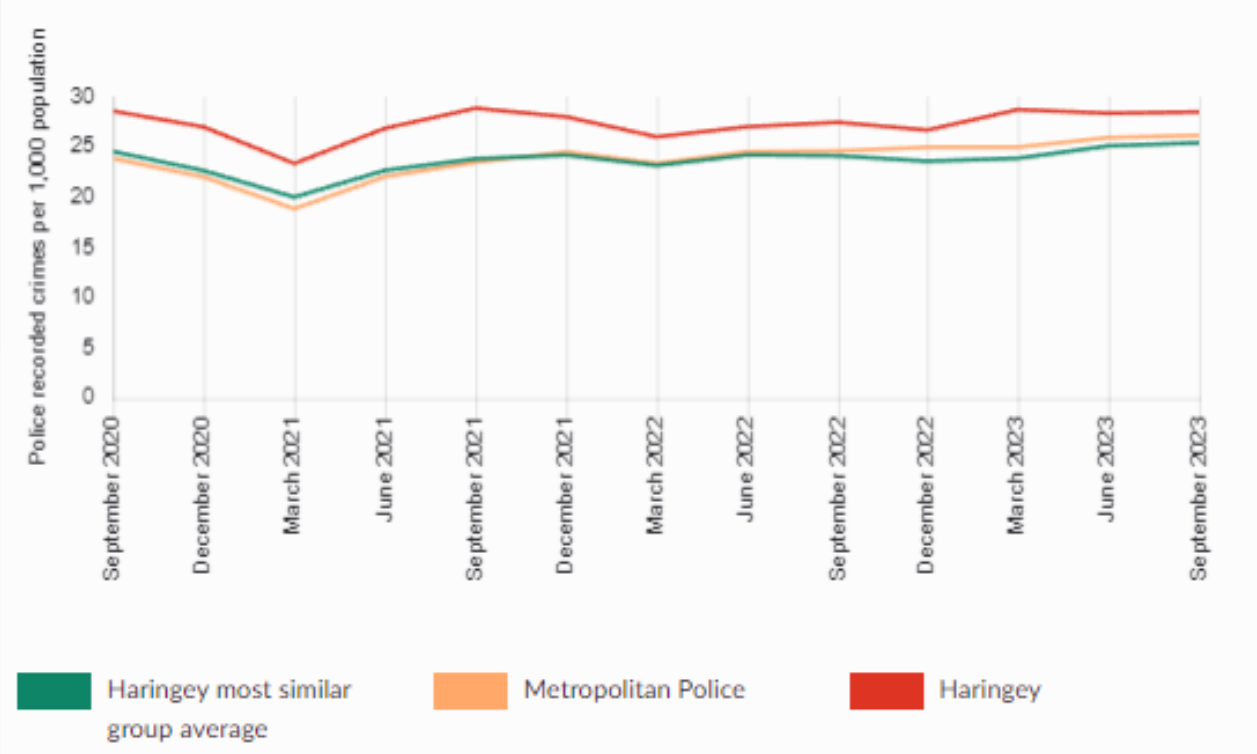

Figure 12 - Crime changes over time in Haringey and the Metropolitan force area.

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