

Crime Impact Statement

Caldershaw Centre, Rochdale



Figure 01 - Proposed Elevation (Source: Archiguma Architects)

Document Control

Job Title:	Caldershaw Centre
Job Number:	CIS46
Report Title:	Crime Impact Statement
Document No:	CIS46-GSL-SY-ZZ-RP-Y-0001-S4-B
Date of Issue:	07-02-2024
Compiled By:	Nasr Haque

Contact

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

Revision control

	Purpose	Date
REV A	Issued for comment.	07-02-2024
REV B	Issued for further comments.	30-02-2025

Table of Contents

1 Executive Summary	3
2 Tenant Security Provision	4
3 Development & Surroundings	5
4.0 Site Survey	6
5 Development Layout & Uses	7
6 Crime Risk Assessment	8
7 Threat Actors:	8
8 Security Design Methodology – Design Basis Threat (DBT)	10
9 Layers of Physical Security: A Comprehensive Approach to Protection	11
10 Security Requirement Statements	12
11 Security Management and Control	13
12 Crime Prevention Through Environmental Design	14
13 Recommendation – Physical Security	15
14 Intruder Alarm	16
15 Access Control	17
16 Internal Video Surveillance	18
17 External Video Surveillance	18
18 Summary	19
19 Appendix	20



1 Executive Summary

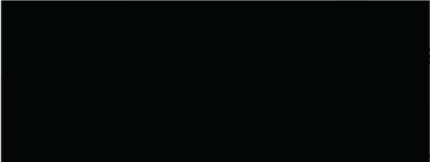
This report describes a Crime Impact Statement (CIS) completed by Graphite Security in support of the design and construction of the proposed Industrial units at Unit 5D Caldershaw Centre, Ings Lane, Rochdale. OL12 7LQ.

This development has been assessed using the principles of 'Crime Prevention Through Environmental Design' (CPTED) in order to identify any opportunities for crime and the fear of crime.

Please note: Rochdale Metropolitan Borough Council may recommend that a planning condition is added that reflects the physical security section of this report.

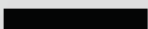
The CIS considers security threats to the proposed development and security vulnerabilities apparent in the architectural designs and proposed use. The CIS follows a security design methodology to provide security recommendations that should be designed and specified in future project stages. These recommendations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

1.1 Security Recommendations



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

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





2 Tenant Security Provision

This report outlines recommendations for ensuring the security and convenience of building tenants, particularly during their fit-out processes, such as the installation of security systems. Whilst it provides guidelines for electronic and physical security measures within each tenant's space, the ultimate decision and responsibility for implementing specific security systems rest with the tenants themselves, based on their individual security risk assessments and operational needs.

The report suggests installing basic security measures around the perimeter of each tenant's area, informed by an initial assessment of potential threats and vulnerabilities. However, tenants are encouraged to conduct their own security evaluations and consider additional enhancements as needed.

Furthermore, the report indicates that the initial security provisions are designed to offer foundational protection, aligning with a standard turn-key fit-out. This foundational approach is intended to facilitate tenants in undertaking more detailed, risk-aligned security enhancements



To support this, the security consultant has included provisions for future enhancements in the initial construction phase, such as ducting and pre-wiring.



3 Development & Surroundings



Figure 02 - Existing Site (Source: Google Maps)

The Caldershaw Centre in Rochdale, located at Unit 5D on Ings Lane (OL12 7LQ), is well-positioned with excellent transportation links, including easy access to major roads such as the A58 and the M62 motorway, public transport options with buses and the Rochdale Railway Station offering regional connections, and proximity to Manchester's extensive network via Metrolink.

[REDACTED] of local amenities, including retail and service establishments within [REDACTED] Rochdale area, along with ample green spaces like Healey Dell Nature Reserve. Educational institutions and a strong community vibe further enhance its appeal.

This combination of accessible transport, comprehensive local services, and a supportive environment presents a solid foundation for both residential and commercial development, highlighting the area's potential for growth and improvement while emphasizing the importance of sustainable practices in future projects.

4.0 Site Survey



Figure 03 - Site Survey (Source: Google Maps + Graphite)

5 Development Layout & Uses

5.1 Proposed Ground Floor Plan

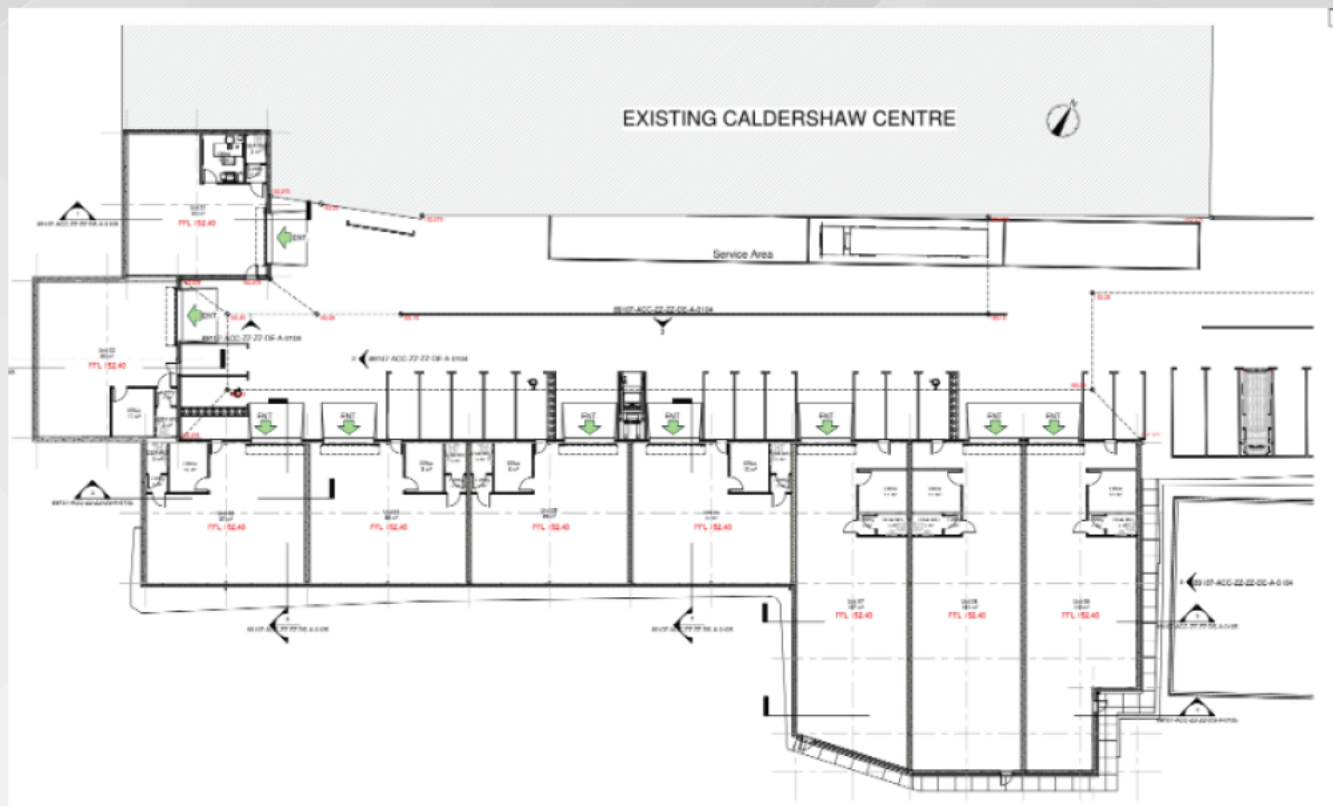


Figure 04 - Proposed Ground Floor Plan (Source: Archiguma Architects)

The buildings is for industrial use. The scheme comprises of nine units, each with a service area. An office space accompanies each unit.

6 Crime Risk Assessment

Warning: Crime Data Missing

Due to an IT systems problem at Greater Manchester Police, data for crime may be missing from July 2019 onwards. The force is working to rectify this issue. In the meantime, we will use previous months allowing us to judge historical crime levels.

Due to the lack of crime recordings from Greater Manchester Police, we have taken the historical crime statistics available from 2018 to 2019.

The **Spotland and Falinge** policing neighborhood, which includes **Unit 5D Caldershaw Centre**, has experienced **higher-than-average crime rates** within Greater Manchester. While GMP has had issues with reporting data post-2019, recent insights indicate that the area continues to experience various crimes, including:

- **Burglary:** There have been multiple recorded incidents of break-ins in industrial and commercial properties. These typically involve forced entry through weak access points.
- **Theft & Vehicle Crime:** This includes theft from commercial units, vehicle break-ins, and theft of high-value goods from industrial estates.
- **Anti-Social Behaviour:** Reports indicate issues such as vandalism, public disturbances, and loitering, which could pose a risk to site security.
- **Graffiti & Vandalism:** Instances of criminal damage and graffiti tagging have been noted in similar industrial areas.
- **Violent Crime:** While not directly relevant to this development, there have been reported incidents of public disturbances in the surrounding area.

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.



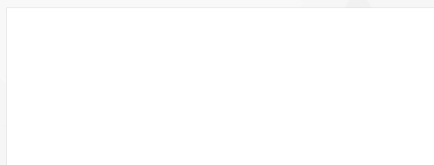
By dissecting the available crime data, we aim to provide valuable insights that can inform the design team aimed at enhancing the safety and well-being of our society.

Based on the information accessible by the police.uk, the crime and disorder in the 'Spotland and Falinge' policing neighbourhood over the past 12 months have been characterised by the following primary categories:

- Violence and Sexual Offences
- Anti-social Behaviour
- Public Order
- Other Theft

For a comparison of graphs between Spotland and Falinge and other areas in Greater Manchester, please see section 19.

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



7 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.



8 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.

8.1 Site-specific DBTs

Attack Category	Description
Opportunistic Theft: Non-Forceful Entry Without Violence	One threat actor endeavours to achieve unauthorized 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.

9 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.

10 Security Requirement Statements

10.1 Caldershaw Centre - Security Requirements Statement

The security requirements for the Caldershaw 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.

11. Security Management and Control

To ensure effective site security, a dedicated **Security Management and Control area** should be provided within the development. This facility will enable **real-time monitoring of access control, intruder alarms, and CCTV**, as well as coordination of **emergency responses**. Given the industrial nature of the site, a **centralised or distributed monitoring approach** may be suitable, depending on operational requirements.

11.1 Recommendations:

- A **Security Monitoring and Control Office** should be incorporated into the site. This space does not need to be a dedicated Security Control Room but must be equipped with appropriate monitoring infrastructure.
- The Security Control Office must be **strategically positioned** with visibility over the main entrance, ensuring staff can **monitor vehicle and pedestrian movements**.
- **Intercom and access control integration** should be provided at all site entry points, allowing for remote access approval and real-time communication with visitors and delivery personnel.
- The Security Control Office should contain a **head-end monitoring station** for CCTV, intruder alarms, and access control.

Response to GMP Comments:

- Addresses **Patrick Babb's concern** about incorporating **CCTV, intruder alarms, and access control infrastructure** from the outset.
-

12. Crime Prevention Through Environmental Design (CPTED)

The development will integrate **Crime Prevention Through Environmental Design (CPTED) principles** to deter criminal behaviour and enhance site security.

12.1 Recommendations:

- **Enhanced site lighting:**
 - High-lumen, **motion-activated LED lighting** to cover all **entrances, service roads, and loading areas**.
 - **Lighting for car parks and rear service areas** to reduce the risk of vehicle crime.
 - **Detector-activated lighting** at doorways and recessed areas to deter unauthorised access.
- **Natural surveillance & access control:**
 - **Minimise blind spots** around loading bays and pedestrian walkways through strategic camera placement and landscaping.
 - Restrict public access to **high-risk areas such as rear service zones** using fencing and gated controls.
- **Territorial reinforcement & signage:**
 - **Clear demarcation** between public, semi-public, and private zones using fences, pathways, and landscaping.
 - **Security signage at entry points**, including **CCTV monitoring and site rules**, to deter potential intruders.

Response to GMP Comments:

- Addresses concerns about **access to rear pathways** by ensuring secure **boundary fencing and gates**.
- Improves **physical security measures** with enhanced lighting, surveillance, and signage.





13. Physical Security

13.1 Boundary Security Recommendations:

- Boundary fencing height to be increased to a minimum of 2100mm, as recommended by GMP.
- The fencing should be close-knit weldmesh or in keeping with the existing palisade boundary, ensuring visibility while preventing climbing.
- Full-height gates at vulnerable entry points, including service pathways and access roads.

13.2 External Door Security Recommendations:

- High-security doors for service areas, including:
 - LPS 1175 Security Rating 2 or LPS 2081 Security Rating B doors for delivery, dispatch, and fire exits.
 - Secure comms, IT, and plant rooms with LPS 1175 SR1 doors.
- All external doors should be self-closing and fitted with heavy-duty locks to prevent unauthorised access.

13.3 Glazing Security Recommendations:

- All accessible ground-floor windows and glass panels must be laminated with a minimum rating of P2A under BS EN 356.
- If P2A is not feasible, use glazing with a PVB interlayer of 0.76mm or greater to improve resistance against impact.

Response to GMP Comments:

- The boundary security now meets GMP's 2100mm fencing requirement.
- Improved glazing standards address concerns that P1A glass may be unsuitable for an industrial setting.





14. Intruder Alarm System

To deter break-ins and improve police response times, an **intruder and duress alarm system** will be installed across all landlord-controlled areas.

14.1 Recommendations:

- **Intruder alarm system to be installed in landlord areas**, with future capability for tenants to expand coverage.
- **Magnetic door contacts** should be installed at **external doors and accessible windows**.
- **Volumetric motion detectors** should be placed in areas where unauthorised access is most likely (e.g., loading bays, entrances, storage areas).
- **Monitored alarm system** with an immediate **response protocol** for security personnel or law enforcement.

Response to GMP Comments:

- Aligns with GMP's recommendation to provide intruder alarms and access control infrastructure for each unit.
- 
-





15. Access Control

A layered access control system will regulate vehicle and pedestrian movement within the development.

15.1 Recommendations:

- **Controlled access at all main entry points:**
 - **Electronic gates for vehicles**, operated via key fob, keypad, or ANPR (Automatic Number Plate Recognition).
 - **Intercom-controlled pedestrian access** to prevent unauthorised entry.
- **Access control for internal areas:**
 - **Staff-only zones** (e.g., back-of-house storage) should be secured with electronic card readers.
 - **Secure access to refuse and cycle storage areas** to deter unauthorised use.
 - **Multi-tenant facilities** should have independent access control to **prevent** cross-access between units.

Response to GMP Comments:

- Ensures all units are designed with future-proofed access control infrastructure, per GMP recommendations.
- 





16. Internal Video Surveillance (CCTV)

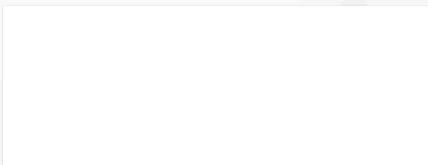
A comprehensive **CCTV system** will cover **key internal areas** to deter crime and assist in incident investigations.

16.1 Recommendations:

- **Fixed internal cameras at all unit entrances**, providing a clear view of doorways and reception areas.
- **High-definition recording capability**, with a **minimum 30-day retention period** for incident investigation.
- **CCTV coverage of shared corridors, loading bays, and key storage areas.**

Response to GMP Comments:

- Addresses the need for **CCTV coverage at entry points and key risk areas.**
-





17. External Video Surveillance (CCTV)

To enhance perimeter security, **external CCTV cameras** will be installed to monitor all access routes and vulnerable areas.

17.1 Recommendations:

- **Fixed external cameras** monitoring **all main entrances and exits**.
- **CCTV coverage** of pedestrian pathways, loading bays, and parking areas to deter vehicle crime.
- **High-resolution cameras with infrared capability** for low-light conditions.

Response to GMP Comments:

- Fully integrates **external video surveillance infrastructure** to align with **GMP's security recommendations**.
-

Conclusion

This revised security strategy directly addresses GMP's concerns by:

- ✓ **Increasing boundary security** (2100mm fencing & secured gates).
- ✓ **Enhancing physical security** (LPS-rated doors & upgraded glazing).
- ✓ **Providing CCTV, access control, and alarm system infrastructure** at all key points.
- ✓ **Improving lighting and environmental design** to deter crime.

These measures ensure the site aligns with **Secured by Design (SBD)** standards while creating a **safe and functional industrial development**.



18 Summary

The security provisions outlined in this **Crime Impact Statement (CIS)** have been assessed against the identified crime risks and tailored to address potential threats specific to the proposed **industrial development at Unit 5D, Caldershaw Centre, Rochdale**. The security measures recommended, including **physical security enhancements, access control, surveillance systems, and Crime Prevention Through Environmental Design (CPTED) principles**, provide a **proportionate and effective** response to mitigate crime-related risks.

The layered security strategy implemented at this site serves to **reinforce physical protection**, ensuring that the development remains resilient to security threats such as **burglary, vehicle crime, and unauthorised access**. The inclusion of **Secured by Design (SBD) principles** further enhances the overall security approach, aligning with **best practices** for industrial development.

This report has been produced based on all **available information**, including but not limited to **site drawing plans, architectural documents, site surveys, environmental visual audits, and consultation feedback**. Should any modifications be made to the **design or build specification**, it is essential that this security assessment is reviewed and updated accordingly to ensure ongoing compliance with security recommendations.

Nasr Haque



19 Appendix

19.1 Crime Data:

Policing Neighbourhood: ['Spotland and Falinge'](#)

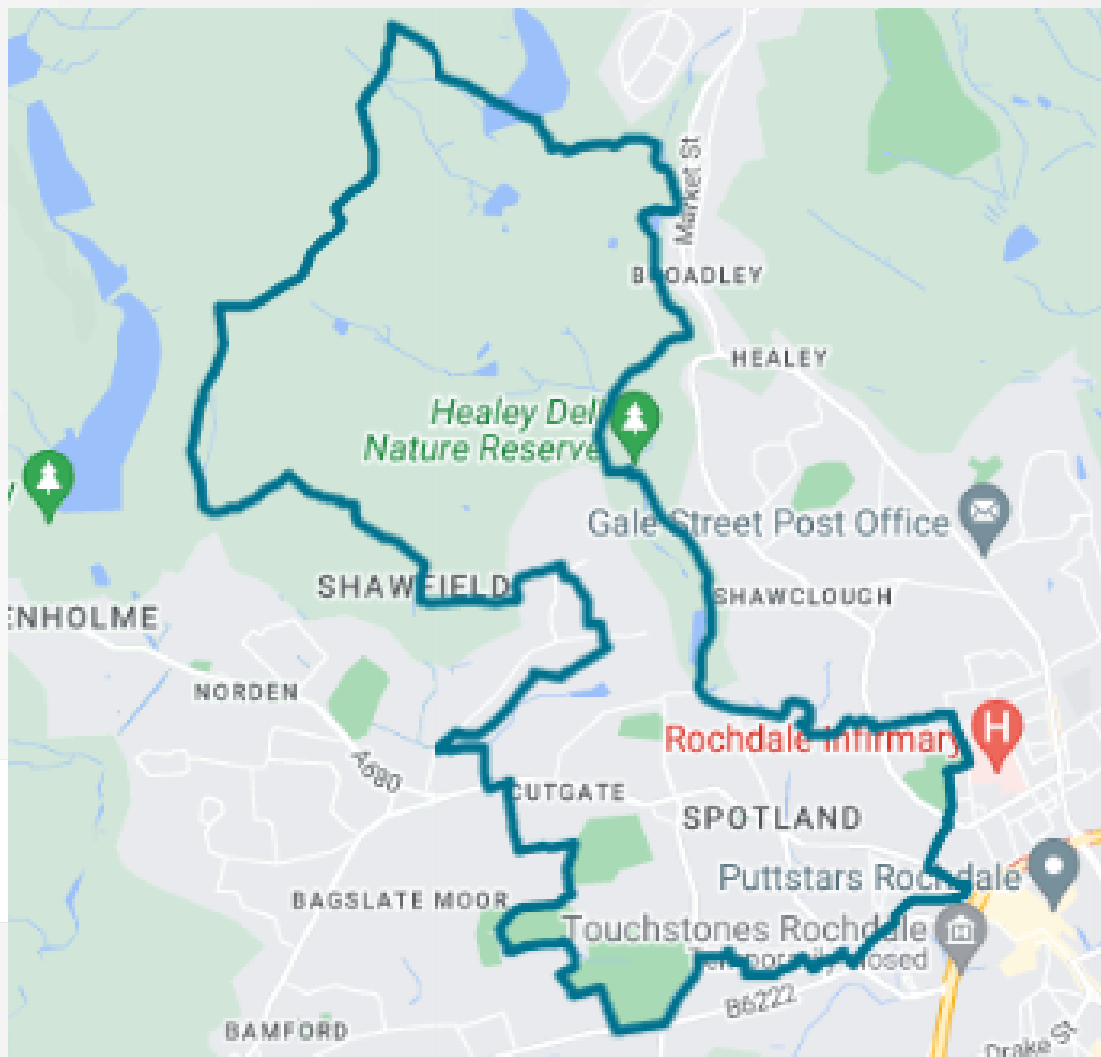


Figure 05 - Area Boundary (Source: Police. uk)



	ASB	Burglary	Robbery	Vehicle	Violent	Shoplifting	CD&A	Other Theft	Drugs	Bike Theft	Theft From the Person	Weapons	Public Order	Other	Total
Jun 2019	23	25	0	28	42	2	17	4	3	2	0	1	16	2	165
May 2019	18	11	0	23	47	3	19	6	1	0	0	3	18	1	150
Apr 2019	23	14	1	23	49	4	24	2	0	0	0	3	19	7	169
Mar 2019	22	14	0	15	71	3	19	10	7	1	1	2	13	5	183
Feb 2019	16	9	2	12	50	5	21	8	1	0	0	0	17	8	149
Jan 2019	24	17	4	20	36	2	31	9	1	0	0	1	21	5	171
Dec 2018	17	14	2	37	47	1	19	4	3	0	0	3	9	4	160
Oct 2018	32	14	3	19	55	9	23	9	1	2	0	1	21	3	192
Sep 2018	25	15	1	23	48	5	15	12	1	1	0	0	13	3	162
Aug 2018	43	7	3	17	48	4	11	6	2	2	1	1	18	5	168
Jul 2018	27	11	2	8	60	9	13	5	4	0	1	6	32	5	183
Jun 2018	52	12	3	7	67	7	19	8	2	2	0	2	30	16	227
May 2018	34	9	1	14	50	4	23	10	0	0	1	0	25	2	173
Apr 2018	23	16	2	12	37	6	15	6	2	1	0	1	18	2	141
Mar 2018	24	11	2	12	47	5	14	10	1	0	0	1	16	7	150

Figure 06 - All crime types in Spotland and Falinge between March 2018 to June 2019.

The crime rate peaked in June 2018 dominated by violence and anti-social behaviour. The lowest recorded crime recorded was in April 2018 dominated by violence and anti-social behaviour.



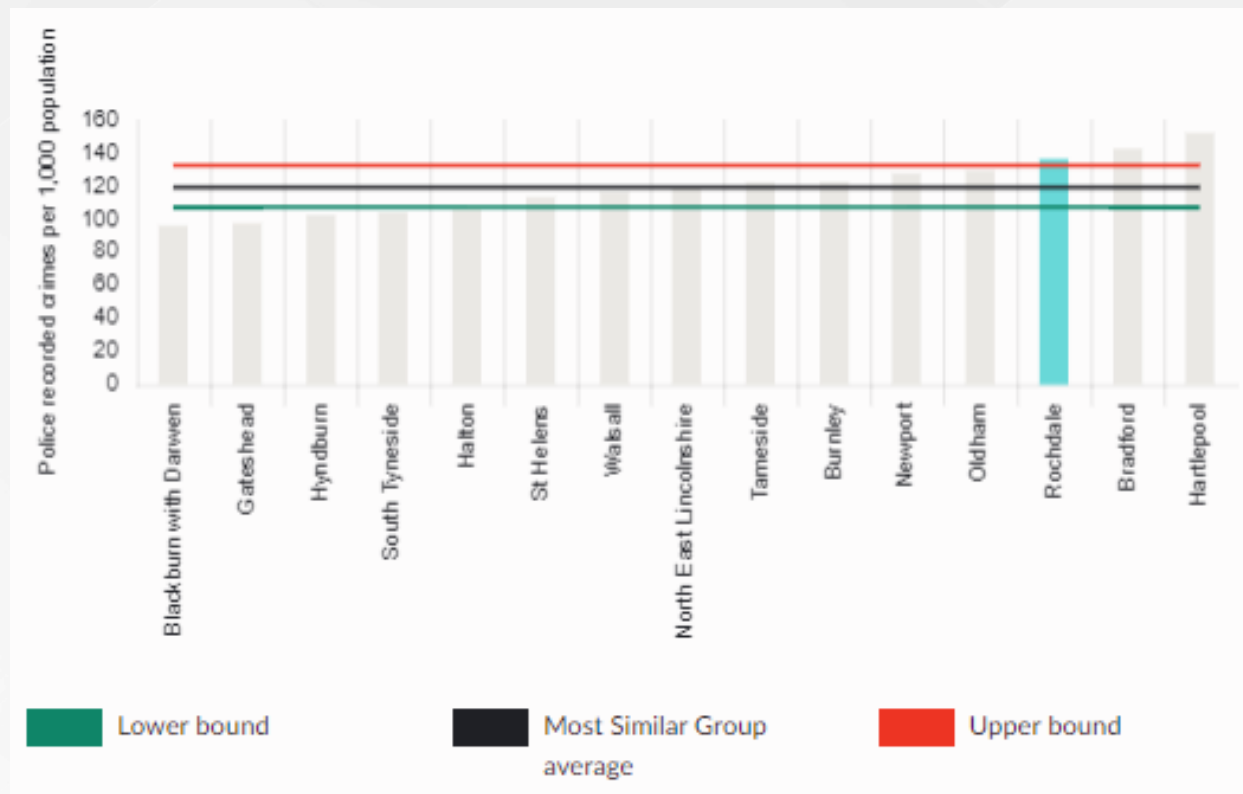


Figure 07 - Crime in Rochdale compared with crime in similar areas (ending in June 2023).

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. Rochdale lies just above the red line, so its crime rate is above the upper-bound group.



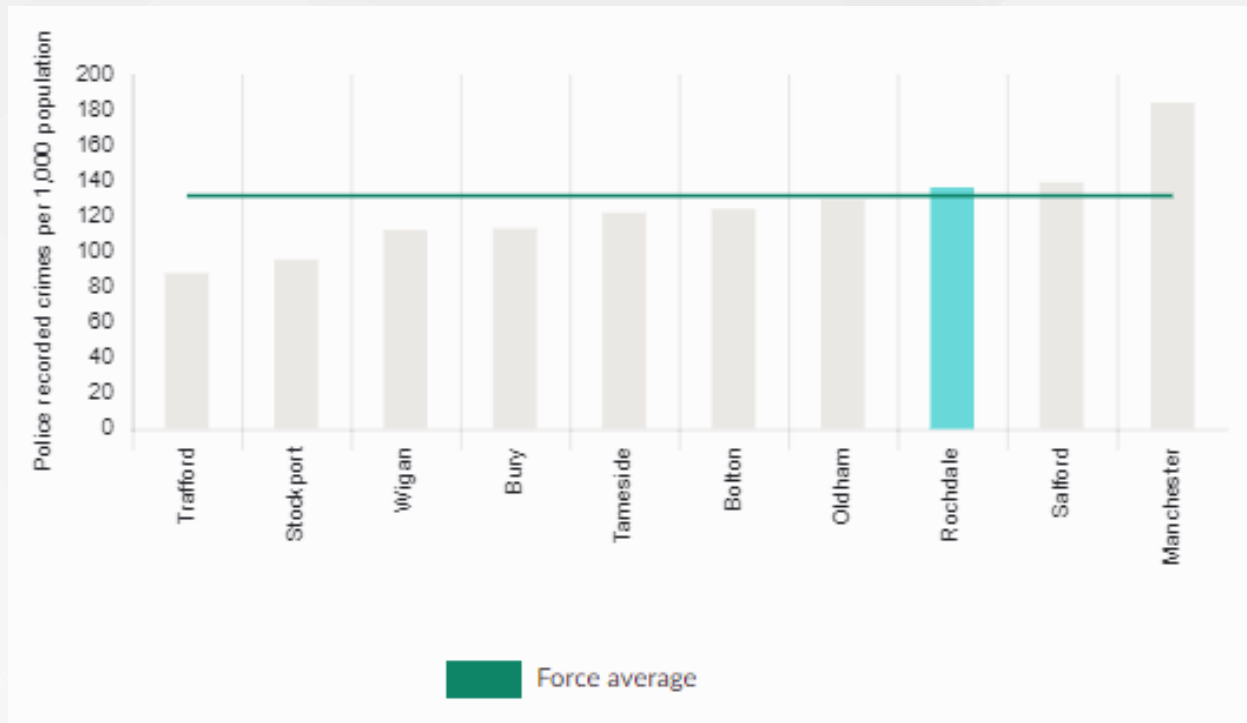


Figure 08 - Crime Stats of Rochdale area compared to Greater Manchester Force Area (ending in June 2023).

The force's average crime rate is 131.05 and the Rochdale area is 136.23 showing it is above the Greater Manchester force average.

The above figure shows all areas within the Greater Manchester Force Area comparing it to the force average crime rate, as you can see Rochdale, where the development is situated is located at the top end of the chart, with Rochdale being the 3rd highest rated area.



In the quarter ending June 2023, crime rates were:

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

Compared with the corresponding quarter in 2022.



Figure 09 - Crime changes over time in Rochdale and the Greater Manchester 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 Rochdale area have changed over time.

