

218 Bury New Road
Manchester
M8 8DY

Our Ref: 2020/0498/CLT/01

F.A.O. Kasbia

6th August 2020

Dear Kasbia,

I refer to your request for a consultation for the above proposal. I have reviewed the development and drafted a short statement highlighting any security-related issues and put together a series of recommendations intended to reduce the risk of criminals being attracted to the locality or the presence of the development being a factor in generating criminal activity.

Observations of the site and surroundings

- Bury New Road has a relatively high footfall. The high footfall includes those walking past and entering the neighbouring buildings. This footfall seems continuous through to the late evening given the location of the development.
- Public transport and regular traffic is prominent past the building.
- The site receives good natural light throughout the day. However, it is unclear on how much natural surveillance the artificial lighting provides on an evening.
- Access onto the grounds of the site is unrestricted with the only boundary treatment being from the neighbouring car parking area.
- The development has been subjected to a ram raid style attack in the past and this was evidenced from the owner and the temporary board which currently sits within the frame of the building.



Risk Assessment

- As the site has no boundary treatment, access to all areas of the site is unrestricted, and whilst on site there were many instances of the public using the site as a cut through to gain access onto Bury New Road without having to take the natural route.
- A public footpath resides in direct proximity to the site and it is overgrown with vegetation which takes away any natural surveillance and provides potential hiding spots for any would be offenders to be able to be undetected obtaining access to the site in the hours of darkness.



View from Bury New Road

- There is no vehicular access gates which provides unrestricted access to the site
- The development has been subjected to criminal damage (as shown below) due to the unrestricted access from multiple points of the site



Recommendations to Improve Security

The following points have been identified for further consideration..

1 Physical Security

In addition to the aforementioned layout issues, the following checklist forms the physical security requirements for this scheme to achieve Secured by Design accreditation.

1.1 Doors

All external doors (single and double leaf) must be compliant with and certified to BS PAS 24:2012, STS02, or LPS 1175 SR2. It is crucial that the door ironmongery to any escape-only doors is permitted under the security certification of the product. All escape-only doors should be alarmed (audible upon opening) and designed without visible external ironmongery

If the main entrance to the building is to be formed by sliding doors, these cannot be certified to the above standards. Any sliding doors should be tested and certified to ENV 1627-30 (WK2+). At the very least, the sliding doors should incorporate laminated glazing, have multi-point locking (preventing sliding and lifting) and be protected by a shutter (certified to LPS 1775 SR2) out-of-hours.

Any shutters / sectional overhead doors must be tested and certified to LPS 1175 SR2. If circumstances could prevent this, please consult with Design for Security.

A robust access control system should be employed, operable by staff swipe card or fob (rather than numeric key pads) preventing unauthorised access to staff-only areas (e.g. through to the workshop from the showroom and up to the staff areas at first floor level). The doors/frames to internal offices/stores should be robust/solid-core (minimum 44mm thick) and capable of being secured when unoccupied. There should be a secure area to allow staff to store their belongings while at work.

Any cash office should have solid masonry walls, no adjacent false/suspended ceilings and a security-certified door-set (see above). A time-delay safe, certified to LPS 1183, is advised and there should be a secure area for the storage of car keys. Staff should only be allowed access to areas required for their work. Keys/passes should only be carried if required for duties and should be accounted for at all times.

1.2 Windows

All windows, where possible, should be certificated to BS PAS 24:2016 or BS 7950. All other window designs/dimensions should take account of the requirements of the above standards, as certified products can carry dimensional restrictions.

Any ground floor and easily accessible opening lights (escape requirements permitting) should be key-lockable, and have fixed/lockable opening restrictors (not releasable from the outside) limited to 100mm.

Any curtain walling panels should include laminated glazing and should be securely fixed directly to the floor slabs where possible, rather than to perimeter columns.

1.3 Glazing

Glazing to a height of 2400mm (or if otherwise accessible) must incorporate at least one pane of glass with a 1.5mm PVB interlayer (e.g. 7.5mm laminated glass), or a glass rated as P4A under EN 356. The remaining pane in a double glazed unit may be toughened glass.

There should be a block work wall or material of similar strength (e.g. welded-steel mesh) behind or within any cladding to the building, to a minimum height of 2000mm from ground level, to ensure that the building fabric itself is not vulnerable to attack.

1.4 Alarms

It is strongly recommended that a monitored alarm system is provided, with a response facility (be that an alert to the key holder, or to a security patrol team). Contacts should be provided on all external doors and PIR detectors should cover all rooms.

Access Control

Access control systems should be operable by swipe card or fob, and not numeric key pads. The following doors should operate on access control:

- Staff only external doors
- Doors into areas restricted to staff
- Storage rooms

1.5 Boundaries

Secure rear boundary treatments should generally be 2400mm high and of welded wire mesh construction. It is recommended that a 358-type fence panel is used in higher risk situations. There should be minimal ground clearance beneath the fence, to reduce the potential for crawling in to secure areas. The site boundary treatment should be positioned on hard standing ground. Where this is not possible, the ground conditions should be reviewed as extra measures may be required to create a secure boundary.

The openly accessible areas of the site should be demarcated by a low boundary and/or indicated by a change in surface treatment to communicate a sense of ownership of the space. Pedestrian access into the site should be well defined.

Perimeter fencing (where exposed to vehicle movements) should be protected on the inner side from potential damage from large vehicles, using crash barriers or rails to deflect any encroachment and therefore maintain a secure boundary.

1.6 Landscaping

In vulnerable locations such as entrances, parking areas and footpaths, low planting should not exceed 1000mm in height, and tree canopies should fall no lower than 2m from the ground. This is in order to allow people to see their surroundings better, make a rational choice of routes and eliminate hiding places. A maintenance agreement should stipulate that these planting dimensions would be adhered to.

Loose surface materials in the publicly accessible areas of the scheme should be avoided. Small fragments of ground covering can be used as missiles against people and premises (both to gain entry and to commit criminal damage).

Planting must be avoided that will aid climbing over boundary treatments. The security of fences can be compromised if trees or street furniture are placed close by.

There should be no hard landscaping that could inadvertently create seating or loitering spots (except within secure designated or otherwise-controlled areas). These features can encourage anti-social behaviour and raise the fear of crime.

1.7 Lighting

External lighting must be provided to pedestrian routes within the site in accordance with BS 5489.

Dusk 'til dawn lights, operated by photoelectric cell/daylight sensor, should be installed to all external doors.

Fittings should produce 'white' light, as opposed to yellow/orange light. Metal halide (or bulbs with a comparable output) should be used, as these offer superior colour rendition over alternatives such as high and low pressure sodium bulbs.

Lighting fixtures must not be positioned to provide climbing aids over boundary treatments. Electrical and architectural layouts should be developed together to avoid this.

1.8 CCTV

Any CCTV system that may be used within this proposal will require certain specifications and intelligent placement of cameras to compliment the design of the development. Designers should consider the following points when planning a CCTV strategy:

CCTV systems (and lighting that support them) require regular cleaning and maintenance to remain effective.

Where necessary cameras that are vulnerable to damage should be protected from attack either by relocation to a higher level and using a bigger lens to achieve the view required or through the fitting of a vandal resistant housing.

With regards to the retention of footage, the police prefer quality over quantity. The overall retention period should be dictated by what the system is designed to achieve, though it would be better to have good quality images over a 14-day period than poor ones over a 30-day period.

Procedures for recovery of recordings are recommended to be established (e.g. trained staff / the CCTV system instruction manual to be readily available). This is to ensure that the images produced will be of an acceptable standard that will allow for identification of an individual which will stand up to scrutiny in court.

Acceptable Standard - this generally requires a resolution of 720x576 pixels at a real time frame rate of 25 frames per second. (N.B. Both the camera and DVR must be capable of this – if the camera will only send low resolution images then it does not matter how high the resolution of the recording unit is).

Identification – One of three levels of field of view. To identify an individual, the image must capture no less than 120% of the field of view (at least from the top of the individuals head to their knees). The remaining two levels of field of view are 'Overview' and 'Recognition', which whilst effective for observational purposes, are less likely to result in the identification of a person/offender.

The intelligent placement of cameras helps to provide clear facial identification of individuals. Suitable locations would be: [Main entrances, gates, vehicle parking area, sales counters and lobbies](#).

In addition to the above, it is highly recommended that any CCTV system has the option of voice alerts (either pre-programmed or live from a monitoring station) to warn any intruders that their actions are being recorded.

1.9 Other

Adequate signage should be deployed in all areas not only to direct people throughout the buildings/sites, but also to deter unauthorised access to certain areas.

Any bin stores should be secure, lockable, and fire resistant enclosures. A strategy should be defined to ensure waste collection can take place whilst retaining a secure development.

Any externally-mounted rainwater pipes should be square in profile and fixed back to the building fabric to prevent climbing to upper floor windows.

Any bollards intended to protect glazed elevations and doors from ram-raid type attacks should use be certified to LPS 1246 or BS PAS 68.

There have been incidents involving metal theft from the area. Consideration should be given to use of alternatives to lead in construction. Avoid exposing cables and use secure inspection covers.

Places that may be vulnerable to graffiti such as expanses of wall and doors should be formed of graffiti-resistant materials or have a protective coating applied at the outset in order to facilitate rapid removal (e.g. 'easy on' – see www.urbanhygiene.com for details).

Management & Maintenance

There should be a comprehensive security regime in place for the day-to-day running of the site. There should be regular reviews/exercises to ensure that it remains accurate, workable and up-to-date. All staff should understand and accept the need for security measures and it should be made easy for people to raise concerns or report observations.

Any high value equipment (e.g. computers, tools, plant/equipment etc.) should be property marked and securely fixed or stored to deter damage/theft. An accurate record should be maintained which logs all such items.

The location of any stored materials or equipment and parked vehicles / trailers within service yard areas can create blind spots that are difficult to survey and obscure the coverage of lighting and CCTV cameras. Good management practises will be essential and consideration should be given to the provision of ground markings to designate where storage is and is not acceptable.

The upkeep of a development over its lifetime can be crucial to the level of security and safety within. Aspects of a development, which are left to deteriorate, have the potential to attract further crime – a process known as 'the broken window theory'. A maintenance plan should be drawn up to address issues such as:

Litter / graffiti removal

- Regular inspection, servicing and repair of security features (lighting, signage, access controls, fencing and gates, alarms, CCTV).
- Trimming and pruning to shrubs and trees

I hope this is helpful and if I can be of further assistance in relation to this matter, please do not hesitate to contact me.

Yours faithfully

Sean Bastow Bsc Hons

Assistant Design For Security Consultant

for and on behalf of Greater Manchester Police| Crime Prevention Team
design**for**security | prevent**and**secure

Office Address: 4th Floor, Greater Manchester Police Force Headquarters, Northampton Road, Central Park, Manchester, M40 5BP

Postal Address: Design for Security, Greater Manchester Police, Openshaw Complex, Lawton Street, Openshaw, Manchester, M11 2NS

T: +44 (0)161 856 5998 | **M:** 07796705135 | **E:** info@designforsecurity.org | www.designforsecurity.org

