Canary Wharf Business Crime Reduction Partnership

PRIVACY NOTICE (OFFENDERS)

This document describes the Scheme, explains why it will process your personal data and the lawful basis for that processing.

It describes the types of processing we will carry out, and the kind of information about you we will process. It also explains how we obtain your personal data, who we will share it with and for how long we will keep it.

At the end of the document, you will be able to read about your rights.

About: Canary Wharf Business Crime Reduction Partnership

We are a membership organisation made up of business owners, or their representatives within the scheme area, Police and Local Authority partnerships and accredited partner Business Crime Reduction Schemes. The purpose of the Scheme is to prevent, detect, or reduce the impact of crime and anti-social behaviour on local businesses within the Canary Wharf Estate and any other Area of Operation.

The Data Controller is Canary Wharf Management Ltd (A subsidiary of Canary Wharf Group).

Contact details

Canary Wharf Business Crime Reduction Partnership
c/o Canary Wharf Group
One Canada Square
Canary Wharf
London
E14 5AB
crime.manager@canarywharf.com

Because the Scheme will process personal data, including your own, it is registered with the Information Commissioners Office. **Z8460599.**

One of the Scheme's obligations under the law is to provide you with all the information you may wish to know about why and how it will process your personal data – and tell you about your rights. This is the purpose of this document.

Please also refer to general privacy notice of Canary Wharf Group plc (CWG). This provides further information to help you understand how CWG collect, use and protect your information when you visit www.canarywharf.com and any other Canary Wharf Group websites and when you visit the Canary Wharf estate in person.

Purpose of processing personal data

The Scheme is a membership organisation which represents its Members who have the right to protect their premises, property, staff and customers from crime and anti-social behaviour, and to exclude from their premises any individuals who are threats to their premises, property, staff, or customers.

Where an individual has been reported by a Member of the Scheme for direct involvement in an incident that represents such a threat, the Scheme will process that individual's personal data for the specific purpose of enabling Members to exercise their rights.

The Scheme's Members will share the personal data of that individual among themselves so that they can identify the individual and may exclude the individual from all the properties of all scheme Members, across the Scheme's Area of Activity which is Canary Wharf Estate, and its surrounding Areas and any additional area as stipulated by the scheme's Board of Management.

You have been reported as involved directly in one or more incidents that represented a threat to one or more Members' premises, property, staff, or customers, and therefore your personal data will be processed by the Scheme on behalf of its Members.

Lawful basis of processing

The Scheme's Members' 'legitimate interest' provides the lawful basis on which it may process specific items of Offenders' personal data for specific purposes without your consent.

The Scheme process Special Category Data under Schedule 1, Part 2 of Data Protection Act 2018 as the Scheme has a substantial public interest in preventing and detecting unlawful acts.

The Scheme also processes alleged or suspected criminal activity under Schedule 1 Part 3 of the Data Protection Act 2018, Paragraph 36 for Substantial Public Interest.

Types of processing

The Scheme undertakes the following types of processing of personal data of Offenders:

- **Data collection**; see **Sources of personal data** below;
- **Data storage**: storage of Offenders' data in a facility independently certified as secure to a high standard;
- **Data retention;** see **Data Retention period** below*;*

- **Data collation**; associating individual Offenders with multiple incidents, and with other Offenders;
- **Data sharing;** as defined in **Recipients, or categories of recipients, of personal data** *below;*
- **Data deletion;** see **Data Retention period** below;
- **Data analysis**; of de-personalised data for historical comparisons etc.

Personal, Special Category and Criminal Activity data

The Scheme may collect the following types of personal data relating to identified and unidentified Offenders:

> Names, Images (Police Custody Images & Members' CCTV Images), date of birth, descriptions, ethnicity, aliases, associates who commit retail crime (including partners), vehicles, arrests, suspected/attempted criminal or anti-social activity, convictions, warning markers, aggravating factors.

Sources of personal data

Offenders' personal data may be provided to the Scheme by:

- **Offenders** who may voluntarily offer information about themselves.
- **Members** who may submit reports about incidents in which Offenders have been involved. They may also send relevant 'intelligence' about Offenders, for example they may provide a name when asked to identify an unidentified CCTV image;
- **Police or other public agencies** may provide Offenders' personal data under a formal Information Sharing Agreement.
- **Data Controllers of other organisations, similar to the Scheme**, in other areas where there is evidence that an Offender has participated, or is likely to participate, in any threat or damage to premises, property, staff and customers in those areas.

Recipients, or categories of recipients, of personal data

The following types of individuals may have access to the Scheme's data, including Offenders' personal data:

- **Members** who are property owners, agents or their employees working within the operational area of the Scheme who share the same legitimate interests;
- **Employees and officers of public agencies** involved in the prevention and detection of crime, such as police, whose lawful basis for processing your data is their public task;
- **Data Controllers of other organisations, similar to the Scheme**, in neighbouring areas if there is evidence that an Offender has participated, or is likely to participate,

in any threat or damage to property, staff and customers in areas outside the Scheme's area of operation.

The Scheme will not transfer Offenders' data outside the UK.

Data retention period of: -

Unidentified Offenders

Unidentified Offenders (e.g. CCTV Images) will be displayed to members for 12 months from the date of the incident unless they are identified sooner. In that case, they may be treated as Targeted or Excluded. If they do not fit either criteria, they will cease to be displayed to members. Once the data has ceased to be displayed to members, it will be retained for 12 months on the Disc Database, only viewable by Administrators and Sub-Administrators before it is irrevocably deleted.

Criteria for Unidentified Offender: Any report by a Member of an Offender whose identity is unknown.

Targeted Offenders

Targeted Offenders data will be displayed to members for 12 months from the date of the incident unless they are identified as being involved in further incident(s). In that case, they may have that 'view' date extended by up to a further 12 months or may be treated as Excluded. If they do not fit that criteria, they will cease to be displayed to members. Once the data has ceased to be displayed to members, it will be retained for a further 12 months on the Disc Database, only viewable by Administrators and Sub-Administrators before it is irrevocably deleted. Where practicable, Targeted Offenders will be issues with a 'Yellow' Warning'.

Criteria for a Targeted Offender: - An Offender who has been reported by a Member, employee and officers of public agencies or other organisations similar to Scheme for direct involvement in an incident that represents such a threat to members of the Scheme.

Excluded Offenders: -

Excluded Offenders data will be displayed to members for 12 months from the date of the incident unless they are identified as being involved in further incident(s). In that case, they may have that 'view' date extended by up to a further 12 months. Once their Exclusion period has ended, they may be reverted to being 'Targeted' for 12 months and their data treated as above. Once they no longer fit that criteria, they will cease to be displayed to members. Once the data has ceased to be displayed to members, it will be retained for 12 months on the Disc Database, only viewable by Administrators and Sub-

Administrators before it is irrevocably deleted. Where practicable, Excluded Offenders will be issues with a 'Red Card' Exclusion for 12 months.

Criteria to Exclude: -

A) Drug dealing, use/possession of a weapon, violent or abusive to store owners/employees/representatives, security, customers or police on arrest or detention, (zero tolerance)

B) Already shown as targeted

C) Already excluded (Liable for exclusion to be extended)

Any person may be Excluded (and issued, where practicable) with a straight 'Red Card' after just one reported incident, especially if that incident involves any form of abuse, threat, violence or discriminatory words or gestures are used against any Business Owner, Staff, contractors, Customers, Police, Council or any member of the Public.

Though the Standard Exclusion is 12 months, Canary Wharf Business Crime Reduction Partnership **may at any time increase any Exclusion period at their discretion**, especially if it involves violence or abuse or repeat offending. **This includes a potential LIFE BAN**. Any rational for variance from a 12 month Exclusion will be recorded within Disc

The Canary Wharf Business Crime Reduction Partnership operates a zero tolerance Policy against such violence or behaviour.

Appeals against Exclusion Notices

An Excluded Person may appeal to the Board against their exclusion. This must be either in writing, or through an online method within 28 days of the date of the exclusion.

The Board will institute a formal appeal process to consider properly submitted appeals.

1. Reviewed by administrator
2. Appeals will be heard by the Board of Management, who will only consider any information submitted in writing or through an online method.
3. The Board of Management in the first instance will consider if the Exclusion has followed the Schemes' Rules and Protocols.
4. The Board of Management can consider any relevant circumstances put before them by the appellant.;
5. A written record of the hearing will be retained.

6. The Board of Management will communicate its decision in writing within 7 days of the decision, either dismissing the appeal, amending the Exclusion period or upholding the appeal.

Age policy

The scheme may share Data of under 18s if they fall into the category of Targeted or Excluded Offenders. However, the Scheme's will not routinely share Data of any unknown person who are or appear to be under 18 unless there are reasonable grounds for doing so and those grounds are recorded within Disc. The Scheme will not display data of anyone who is or appears to be under the age of 12. However, the scheme may process that Data and pass it to appropriate authorities (Police/Council) for appropriate action. The Scheme may store Data of Under 12s in the Disc Database but this data will only be accessible to the Scheme's Administrator and Sub-Administrators, subject to the Scheme's policy on Irrevocable Erasure of Personal Data (*see below*)

Data may also be shared by consent. e.g. In the case of a Missing Person under 18 years old and consent to share data has been authorised by a parent or guardian. This includes persons Under 12 years old.

Your rights

You have the right to obtain a copy of all the personal data which the Scheme holds about you; to do so the Offender must contact the Data Controller (see contact details above); you may be required to provide proof of your identity. In any case the Scheme will respond to your request within 30 days.

If, when you access your personal data, any of it is found to be incorrect, unnecessary, or disproportionate, you can require the Scheme to correct it. You do not have the right to require the Scheme to delete any data which is correct, necessary or proportionate for the Scheme's purposes of processing.

You have the right to complain about the Scheme to the Information Commissioners Office; you can submit a complaint on the ICO's website at https://ico.org.uk/concerns/handling/