Bexleyheath Together

(the Scheme)

RULES & PROTOCOLS

This document, the *Rules & Protocols* of *Bexleyheath Together* ('the 'Scheme') describes the obligations of Members of the Scheme.

Before becoming a Member of the Scheme, and before accessing any Scheme data, all prospective Members must certify that they have read, understood, and agreed to abide by this document. Access to the Scheme's data will not be given to any Member who does not first certify that they have read, understood, and agreed to abide by this document.

This document is always available to view or download from the Scheme's Disc system.

Contents of this document

Name, address and contact information of the Scheme:

Bexleyheath Together
Bexleyheath Business Partnerships Ltd
Broadway Shopping Centre
Management Suite

Bexleyheath
DA6 7JN
info@bexleyheathbid.co.uk

Criteria of Membership

Membership of the Scheme is restricted to:

- Levy-Payers, owners, or their representatives, of private property or other private facilities open to the public in the Scheme Area (see below);
- officers of public agencies statutorily tasked with the prevention and / or detection and / or reduction of crime and / or anti-social behaviour in the Scheme Area (see Scheme Area below)
- Administrators or Sub-Administrators of Partner schemes who share a similar legitimate interest

Scheme Area

The Scheme Area is Bexleyheath BID area and/or any other area that the Board of Management decide upon.

The Scheme's Members-only Website and App *('the Scheme's Disc system):*

The Scheme's Website (the Disc Desktop) web-address or URL is: https://www.disc-net.org/bexleyheath

The Scheme's App (the Disc App) can be downloaded from the AppStore and Google Play Store etc.

Only Members who have been sent a Welcome email from the Scheme and have completed the certification process which is accessed through the Welcome email can access the scheme's Disc system, and the data which is there.

Members obligations under current Data Protection law

The Scheme captures, processes and shares amongst its Members 'Personal Data' relating to persons reported to the Scheme. Use of this data is carefully regulated by current data protection law. To ensure compliance with the law, Members are obliged:

1. to keep all information received through the Scheme confidential and not to disclose it to any third party, either directly or indirectly, unless required to do so by law or by the

order or ruling of a Court or Tribunal or regulatory body;
2. not to print any Personal Data from the Scheme's Disc system;
3. not to copy any Personal Data from the Scheme's Disc system into any other system;
4. to submit Incident Reports on persons by using the secure online facilities available through the Scheme's Disc system;
5. to ensure that information on the Scheme's Disc system is only accessed by or disclosed to other Members of the Scheme;
6. to ensure that appropriate security measures are employed to prevent unauthorised access to, or alteration, disclosure or destruction of Personal Data provided through the Scheme's Disc system;
7. to allow the Scheme to audit each Member's compliance with the above obligations;
8. to ensure that, where relevant, the Member's employer organisation is compliant with current data protection law.

Members' participation in the Scheme's Disc system

When a Member observes a person in an act which represents a threat to the Member's premises, property, staff or customers, the Member agrees to submit an Incident Report through the Scheme's Disc system about the event as follows:

1. where the person is displayed on the Scheme's Disc system, to make Incident Reports by clicking or tapping on that person's facial image or name as displayed in the Disc system;
2. where the person is not displayed on the Disc system, to use the appropriate Incident Report form on the Disc system to submit as much personal information about the person as may be required by other Members in order to identify the person, and to indicate on the Incident Report if the person is known to the Member.

General Description of Technical & Organisational Security Measures for Personal Data

Technical security: All personal data will be processed within the Disc system; the security provisions of the Disc systems are described in the document *Littoralis & Disc Data Security & Protection Provisions*; Members can access the Scheme's data only through the Disc Desktop and/or Disc App.

Organisational security: where it is necessary for personal data to be stored temporarily outside the Disc system, the Scheme will do so, where possible, in an encrypted format and/or in a password-protected manner. Where this is not possible, for example where data is held in hard-copy (paper-based), all such data must be secured in a locked cabinet and access will be through the Scheme administrator or a

duly authorised deputy or a member of the Board of Management.

Personal Data will be permanently erased (digital) or destroyed (eg paper-based) in compliance with the Retention & Erasure policy defined in the Scheme's relevant Privacy Notice(s).

The Scheme

Unidentified Persons [ID Sought]

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

The scheme may display images on galleries for 6 months of unidentified person [ID Sought] who have committed crime and/or anti-social behaviour against a members' business.

If identified, that subject will be removed from the unidentified gallery treated as a potential Target Person. If they do not fit that criteria, they will no longer be shared with Members.

Targeted Persons

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 Offender

The Scheme may display names and/or images of 'Targeted Persons' on the Scheme's Disc system. These persons have either been subject to at least a single Incident Report for criminal or anti-social behaviour by Members or their personal information has been supplied to the Scheme by an authorised Partner (eg police) for sharing with Members. These persons are not excluded from Members premises.

The purpose of displaying Targeted Persons on the Scheme Website is to:

- ensure that such persons are aware that the Scheme knows their identity, and thus to encourage them to desist in any further criminal or anti-social behavior in the Scheme Area;
- enable Members to be aware of, and easily identify, persons who are or have been recently active in low-level crime and/or anti-social behaviour and, where

necessary, submit Incident Report(s) about relevant behaviour.

Unless a Targeted Person becomes subject to an Exclusion Notice (*see below*) his/her Personal Data will be withdrawn from display on the Scheme Disc system after 12 months. This data will continue to be accessible in the Disc database only to the Scheme's Administrator and nominated Members with full Administrator rights subject to the Scheme's policy on Irrevocable Erasure of Personal Data (*see below*)

The term 'Targeted Persons' will reflect all categories of displayed Galleries to members other than Unidentified persons [ID Sought] and Excluded.

Excluded Persons

Criteria to Exclude: - Violent or abusive to owners/employees/representatives, Security, customers or Police on arrest or detention (Zero Tolerance). Already Displayed as 'Targeted'. Already displayed as 'Excluded'

The Scheme may maintain one or more lists or galleries of Excluded Persons.

Excluded Persons

1. If a person has been subject to 2 Incident Reports relating to retail-related crime and/or anti-social behavior within a 12 month period submitted by any Member or authorized partner (i.e. Police), the Scheme will serve an Exclusion Notice on this person, thus designating him/her as an Excluded Person who is excluded from the premises of all Members of the Retail Scheme.

2. The length of exclusion is 12 months and will become effective from the date of the latest relevant incident reported.

3. If an Excluded Person is subject to an Incident Report submitted by a Member during the period of his/her exclusion, that period of exclusion is extended by 12 months from the date of the latest incident reported.

4. As soon as an Excluded Person completes his/her period of exclusion, all Personal Data will be removed from the Disc system. If the Administrator believes there is justification for retaining it as a Targeted Person (see 'Targeted Persons' above) his/her information will be managed accordingly and the Data Controller must record a rationale for this extension and note it on the Targeted Person's file in Disc.

5. The scheme will endeavor to serve individuals with a Banning Letter (Exclusion Notice). However, where this is not practicable, they may still be Excluded without notice being served.

6. The above conditions will be reflected within the scheme's Privacy Notice for Offenders.

Unless an Excluded Person becomes subject to a further exclusion period or there is justification for retaining as a Targeted Person (*see above*) his/her Personal Data will be withdrawn from display on the Scheme Disc system (ie will no longer be shared with the Scheme's Members) after 12 months.

This person's data will continue to be accessible in the Disc database only to the Scheme's Administrator and nominated Members with full Administrator rights in accordance with the Scheme's policy on irrevocable deletion of Personal Data (*see below*)

Irrevocable deletion of Personal Data

All Personal Data pertaining to any person will be irrevocably deleted from the Scheme's database 12 months (Unknown Offenders for 6 months) after either the last expiry date of any applicable exclusion scheme or the last incident reported relating to the said person, whichever is the latest. Until that time, this data will continue to be accessible only to the Scheme's Administrator and nominated Members with full Administrator rights.

Relevant anonymized (previously Personal) Data will be retained only for historical statistical analysis.

Sharing Personal Data

The Scheme may share Personal Data of a person only:

1. where the receiving Scheme complies with Good Practice to a level comparable with that defined in this document;
2. where the receiving Scheme shares the same or similar Common Purpose as the Scheme;
3. where Personal Data to be shared is not subject to restrictions of use which preclude such sharing;
4. where the receiving Scheme notes and retains a rationale justifying the acquisition of the Personal Data (for example, that the person is likely to travel to the receiving

Scheme area).

Subject to agreement of the Board of Management of the Scheme, the Scheme may share Personal Data stored in its database with suitably authorised third-party organisations such as police, other Scheme Administrators etc.

Where Members wish to share data with the Scheme subject to additional conditions they may draw up additional Information Sharing Agreements with the Scheme's Board of Management

Ownership and rights of use of images

When a Member submits an image of a person to the Scheme either through the Disc system or through any other method, the Member grants the Scheme full use of the image in accordance with this document, confirms that the image has been obtained in compliance with current Data Protection law and the CCTV Code of Practice, and where relevant asserts his/her ownership of the image, and right to grant usage of it by the Scheme.

In the case of unidentified images of persons, the submitting Member grants the Scheme unlimited rights to share the image with other Schemes and authorised third parties for identifying the person displayed.

Data Subject Access Requests

Persons may request access to all and any of their person data processed by the Scheme by means of a Data Subject Access Request and require correction of any data that the persons can show to be incorrect; information on how to submit Subject Access Requests is included in the Scheme's Privacy Notice which is provided to all persons where possible or, only where not possible, made as widely accessible and available as possible to them.

Appeals against Exclusion Notices

An Excluded Person may appeal to the Board against his/her exclusion. This must be either in writing, or through an online method.

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

1. appeals will be heard by the Board of Management, who will only consider any information submitted in writing or through an online method.
2. the Board of Management in the first instance will consider if the Exclusion has followed the Schemes' Rules and Protocols.
3. the Board of Management can consider any relevant circumstances put before them by the appellant.;

4. a written record of the hearing will be retained.
5. 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.

Other obligations

In addition to the above obligations, Members are obliged to:

1. maintain their contact information on the Scheme's Disc system and ensure that it is correct;
2. refer any formal complaint by a person displayed on the Disc system regarding any element in the Disc system or administrative processes or procedures to the Scheme Administrator via the Disc system;
3. be aware that all data accessible on the Scheme Disc system is the property of the Scheme except where otherwise stated.