**Privacy Notice**

**Bluewater Business Against Crime**

PRIVACY NOTICE (OFFENDERS)

This document describes Bluewater Business Against Crime (the Scheme), explains why the Scheme processes the personal data of specific individuals (Offenders) and the lawful basis for that processing. It describes the kind of information about Offenders that the Scheme processes and what it does with that information.

**Contact details**

Bluewater Business Against Crime

Bluewater Shopping Centre

Upper Rose Gallery

Bluewater

Greenhithe

Kent

DA9 9ST

Email address: dataprotection@landsec.com

Tel:  01322 475475

The Scheme’s Data Controller is responsible for ensuring its compliance with current Data Protection law and can be contacted at the above address, email address or telephone number. The Scheme is registered with the Information Commissioners Office as a Business Crime Reduction Partnership (registration Z1262078)

 This statement confirms Bluewater Business against crime’s (BBAC) commitment to protect your privacy and to process your personal information in a manner which meets the requirements of the General Data Protection Regulation (GDPR May 2018), previously the Data Protection Act (1998).

Bluewater Business Against Crime (BBAC) is a membership organisation established to assist member businesses to respond in an organised manner to crime that affects their businesses, profitability, staff, customers and the local economy. By working together and sharing information about crime and those committing it, the partnership provides greater protection for its members.

The partnership is registered with the information commissioner for the purpose of ‘the prevention and detection of crime and the prosecution of offenders’.

**Purpose of processing personal data**

Members of the Scheme have the right to protect their property, staff and customers from crime and anti-social behaviour and to exclude from their premises any individuals who are proven threats to their property, staff or customers. The Scheme processes Offenders’ personal data for the specific purpose of managing its Exclusion Scheme on behalf of its Members.

The Scheme’s area of operation, and its Exclusion Scheme, extends across Bluewater shopping Centre, its road network and lakes. A copy of the area will be provided in any correspondents.

**L****awful basis of processing**

**Offenders**

The Scheme’s Members’ ‘legitimate interests’ provides the lawful basis on which it may process specific items of Offenders’ non-special category personal data.

For special category data, such as ethnicity, or for criminal offence data, the processing is based on Substantial Public Interest and DPA 2018 Schedule 1 Part 2 processing for the purposes of preventing or detecting unlawful acts. As long as the processing is necessary for the purpose, consent of the data subject is not required if this would be prejudice the prevention or detection of the unlawful act.

**Members**

Personal data relating to Members is processed to fulfil a contract between the Bluewater Business Against Crime and its members.

**Categories and types of personal data processed**

**Offenders**

* **Offender’s name and facial image and any relevant information about the nature of his/her activities**; the purpose of this processing is to enable Members to identify Offenders in order to submit reports about them, to include them in a list or gallery of excluded persons (if appropriate and in line with the Scheme’s Rules & Protocols), and to provide information about them which may be necessary to protect the personal safety of Members and their staff, customers etc. This data may be shared among Members;
* **Offenders’ postal and email addresses, telephone number(s) and other contact details**; the purpose of this processing is to enable the Scheme to communicate with Offenders from time to time, for example to send confirmation of exclusions, rules of the exclusion scheme, or confirmation that exclusions have expired. Such data will not be shared with Members;
* **Offenders’ ethnicity**; this is special category data and we will process this only to assist our Members to identify a known Offender in order to submit a report about an incident in which they have been involved, or to identify prolific or travelling offenders;
* **Information and evidence about incidents in which an Offender has been involved**; the purpose of this processing is to enable the Scheme to defend its legal rights against any claim or suit by an Offender or other party. Such data will not be shared with Members but only with the Scheme’s Data Controller and Board of Management as necessary in the course of any legal proceedings.

**Members**

Name, place of employment, postal and email addresses, telephone and other contact details

**Sources of personal data**

**Offenders**

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.

**Members**

Current agreements. Members may also update their information as needed.

**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, or data processors, 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**

**Offenders**

When an Offender is reported by a Member for participating in any threat or damage to any Member’s property, staff or customers, his/her name and facial image may be shared among Members for 12 months. If no further report is submitted during that period, the Offender’s data will be withdrawn from Members at the expiry of that period. It will be retained for a further 12 months in the Scheme’s database (which can only be accessed by the Data Controller) after which time it will be irrevocably deleted.

If during the 12 months when an Offender’s data is circulated among Members he/she is reported for another incident involving a threat or damage to any Member’s property, staff or customers, his/her name and facial image will be circulated among Members for a further 12 months from the date of the second report. **Additionally, the Offender will be excluded from all the properties of all Members for 12 months, and this fact will be shared with Members.** If no further report is submitted by a Member during that period, the Offender’s data will be withdrawn from Members at the expiry of that period. It will be retained for a further 12 months in the Scheme’s database (which can only be accessed by the Data Controller) after which it will be irrevocably deleted.

**Members**

The personal data will be retained for as long as the members remains a Member of the scheme. In the case of submitted reports, the submitting Member’s email address only will continue to be associated with suchas reports for as long as the report is retained by the scheme.

**Security**

The scheme processes all personal data within the DISC online ‘secure environment’. The DISC system aligns with the principles of “Data Protection by design and default”.

**Rights**

You have the right to opt out of receiving any marketing information which we send you.

**Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

**Your rights in connection with personal information**

Under certain circumstances, by law you have the following rights:

 • Subject to certain conditions, request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. If possible, you should specify the type of information you would like to see to ensure that our disclosure is meeting your expectations. Disclosure should not impact the rights and freedoms of other people, e.g. privacy and confidentiality rights of other staff.

• Subject to certain conditions, request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. You also have a responsibility to help us to keep your personal information accurate and up to date. We encourage you to notify us of any changes regarding your personal data as soon as they occur, including changes to your contact details. This right only applies to your own personal data. When exercising this right, please be as specific as possible.

• Subject to certain conditions, request erasure of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. We may not be in a position to erase your personal data, if for example, we need it to (i) comply with a legal obligation, or (ii) exercise or defend legal claims. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below).

 • Subject to certain conditions, object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

• Subject to certain conditions, request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

• Subject to certain conditions, request the transfer of your personal information to another party. If you exercise this right, you should specify the type of information you would like to receive (and where we should send it) where possible to ensure that our disclosure is meeting your expectations. This right only applies if the processing is based on your consent or on our contract with you and when the processing is carried out by automated means (i.e. not for paper records). It covers only the personal data that has been provided to us by you.

Where our processing of your personal data is based on your consent you have the right to withdraw your consent at any time. If you do decide to withdraw your consent we will stop processing your data for that purpose, unless there is another lawful basis we can rely on – in which case, we will let you know. If you withdraw your consent, this will only take effect for future processing.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please email dataprotection@landsec.com

You will not have to pay a fee to access your personal information (or to exercise any of the other rights); however, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

You can also contact the Information Commissioner's Office via <https://ico.org.uk/>  for information, advice or to make a complaint.

**Links to other websites**

There are hyperlinks within this website which will take you away from the DISC website. The linked sites are not under the control of BBAC and we are not responsible for the content of any linked site or any link contained in a linked site, or any changes or updates to such sites.

**Disclaimer**
The BBAC partnerships seeks to ensure that all information on this website is accurate However, we do not accept any responsibility or liability for any claim, loss or damage whatsoever from the use of any information within, or accessed through, this website.

# Cookies

The website only contains Strictly Necessary Cookies. These cookies are necessary to operate our Online Services. They do not store any personally identifiable information. You can set your browser to block or alert you about these cookies, but our Online Services will not work properly without these cookies.

# CHANGES TO THE PRIVACY & COOKIES POLICY

This Privacy Notice was last updated on 19 February 2019. If it is necessary for us to alter the terms of the Privacy Notice, we will post the revised Privacy Notice here. We encourage you to frequently review the Privacy Notice for the latest information on our privacy practices.