

## **Bristol BCRP (The Scheme)**

### **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: Bristol BCRP**

We are a membership organisation made up of owners, or their representatives, 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, low-level crime and anti-social behaviour on local businesses within the Bristol BCRP Area and/or any additional area that the Board of Management may decide.

#### **Contact details**

##### ***Bristol BCRP***

*Office 1.05, 1 Victoria Street, Redcliffe, Bristol*

*BS16AA*

*Email address: [carmen.ceesay@visitwest.co.uk](mailto:carmen.ceesay@visitwest.co.uk)*

*Tel: 07715523215*

Because the Scheme will process personal data, including your own, it is registered with the Information Commissioners Office (Registration Number: - **Z6790025**)

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.

#### **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 the Bristol BCRP Area, or 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.

### **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 14. 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 14s 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 14 years old.

### **Missing Persons**

Details of Missing Persons, including images, that are officially reported to Police, may be shared with members. Notification will come from Police and will only be shared by consent on Police authority. Once that person has been located and is no longer classified as 'missing', their details will be removed from the Gallery as soon as possible, unless it is appropriate that they are still classed as 'Targeted' and there is justification to continue sharing, processing, or storing their data under Legitimate Interest.

## 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.

## Incident Retention Period

Bristol BCRP will only retain Incident Data for 3 years from the date of submission. All incident data is then anonymised and only retained for analytical purposes.

## **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 Gallery view period 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.

## **Data retention period of: -**

### **Unidentified Offenders**

Unidentified Offenders (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 12 months on the Disc Database, only viewable by Administrators and Sub-Administrators before it is irrevocably deleted.

**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 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’

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 them 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 their 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 their 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) their 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*) their Personal Data will be withdrawn from display on the Scheme Disc system (i.e. 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*)

## **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/>