SAFER YORK BUSINESS PARTNERSHIP (SYBP) EXCLUSION SCHEME

PRIVACY NOTICE (OFFENDERS)

This document describes the Safer York Business Partnership Exclusion Scheme (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

Safer York Business Partnership

C/O Safer York Partnership
2nd Floor
West Offices
Station Rise
York
YO1 6GA
Email address: info@saferyorkbusiness.org
Tel: 07714618150

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.

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 the City of York area.

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.

Lawful basis of processing

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

The Scheme has assessed the impact of its processing on Offenders' rights and freedoms, has balanced these with its Members' own rights, and has concluded that its Members' rights prevail over Offenders' rights in this specific matter. Therefore, for the specific purpose of managing an exclusion scheme, Members' legitimate interests constitute the Scheme's lawful basis for processing Offenders' personal data without requiring consent.

Categories and types of personal data processed

Offender's name and facial image and any relevant information about the nature of his/her activities held in the Sentry Secure Information System (SentrySIS);

- For the purposes of the prevention of crime and detection of unlawful acts, SentrySIS holds personal data about Subjects of Interests. SentrySIS does not ask Subjects of interest for consent to process their personal data as this prejudice these purposes.
- SentrySIS users, including police personnel upload information about Subjects of Interest only when that individual is reasonably suspected of crime or unlawful acts.
- The uploading of Subjects of Interest is strictly controlled and any SentrySIS user who uploads any data which is not compliant and in line with the SentrySIS EULA and other documentation, could be subject to fines or censure by the SentrySIS business subscribers, the crime partnership, the local authority, the police constabulary or business improvement district they are employed by or are members of. They could also be subject to fines or censure from the Information Commissioners Office.
- SentrySIS Users are data controllers of all the data they upload within the SentrySIS system. SentrySIS helps facilitate the sharing of Subject of Interests' personal data between SentrySIS Users, Business Subscribers, Local Authority Personnel and The Police, through acting as the data processor.

- Subject of Interests' personal data comprises of the following:

  1. Their Name
  2. Their Gender
  3. Their Ethnicity (Special Category Data)
  4. Their Date of Birth
  5. Their Eye Colour
  6. Their Physical Build
  7. Any other names they might be known as
  8. Any distinctive marks or appearance they may have
  9. Images of their face (Special Category Data)
  10. Images of their body
  11. Their facial recognition ID (Special Category Data)
  12. Dates and times of incidents they have been suspected to have been involved in
  13. The incident crime category which they have been suspected to have been involved in

No other sensitive or 'special category' personal data (sexuality, religious beliefs etc) is processed by the Scheme.

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;
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.

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.

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

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.

Offenders' rights

Every Offenders has the right to obtain a copy of all the personal data which the Scheme holds about him or her; to do so the Offender must contact the Data Controller (see contact details above); the Offender may be required to provide proof of his/her identity. In any case the Scheme will respond to the request within 30 days and provide full documentation to demonstrate compliance with Data Protection law.

Online Subject Access Requests can be made at www.saferyorkbusiness.org

Written requests should be addressed to at the address at the top of this document.

If, when an Offender accesses his/her personal data, any of it is found to be incorrect, unnecessary or disproportionate, the Offender can require the Scheme to correct it. Offenders do not have the right to require the Scheme to delete correct, necessary or proportionate information.

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