



**SAFER YORK
BUSINESS
PARTNERSHIP**

DATA INTEGRITY STATEMENT

The Data Protection Act 2018 regulates the obtaining, storing, processing and disclosure of personal data about living persons. All processing must be in compliance with the provisions of the act and in the event of non-compliance the Information Commissioner may take enforcement action.

Particular obligations are placed upon the partnership, its members and the data controller and you, as a member of the partnership, must comply with the Data Protection Principles governing the act.

The Data Protection Principles state:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to Individuals
2. Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Personal data shall be accurate and where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
5. Personal data processed for any purpose or purposes shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental; loss, destruction or damage, using appropriate technical or organisational measures.

In addition, GDPR provides eight rights for Individuals: -

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

The partnership is an initiative operated by business in partnership with police and other agencies and organisations, through an agreement with each of the members, who have agreed to the principles set out in the partnership documentation and protocols.

The partnership Board of Management is the data controller and is responsible for all matters concerning the management of the partnership. The BoM will determine the purposes for which, and the manner in which, any personal data is or is to be, processed.

Data shall be kept secure. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Personal data consists of information relating to a living individual, who can be identified from that information. Personal data shall be processed in accordance with the rights of data subjects under this act.

A Data Subject is a living individual who is the subject of personal data.

Data means information which:

- a) I being processed by means of equipment operating automatically in response to instructions given for that purpose.
- b) Is recorded with the intention that it should be processed by means of such equipment.
- c) Is recorded as part of a relevant filing system, or with the intention that it should form part of a relevant filing system, or;
- d) does not fall within paragraph a), b) or c) but forms part of an accessible record.

Processing in relation to personal data, means obtaining, recording or holding information or data or carrying out any operation in relation to the information or data, including:

- Organisation, adaptation or alteration of the information or data.
- Retrieval, consultation or use of the information or data.
- Disclosure of the information or data by transmission, or otherwise making available.
- Alignment, combination, blocking, erasure or destruction of the information or data.

Any person who collates, manages, distributes or receives or views files, photographs, information or other personal data about a living person is a data controller.

The partnership crime manager is part of the data controller function of the partnership and is not a data processor.

Disclosure of personal data about a data subject to members of the partnership will be approved by the data controller only when it is relevant to the purposes of the partnership and it is lawful to do so, taking into account the Data Protection Principles.

Disclosure of data to members will relate to:

SYBP Data Integrity Statement

V4 - 161023

- The prevention and detection of crime
- The apprehension or prosecution of offenders or suspected offenders.
- Person(s) who are identified by the partnership as target criminals.

A target criminal is a person whose behaviour is persistently criminal or anti-social and will include:

- A person who is known, from reliable information, to be actively involved in committing or attempting to commit crime or anti-social behaviour in or near the operational area.
- A person who has been convicted within the previous 12 months of a criminal offence.
- A person living in or near the operational area who has been convicted within the previous 12 months of a criminal offence.
- Any person who has been served with an exclusion notice preventing him/her from entering any member premises.
- A person who is on bail for any criminal offence.
- A person subject to a Criminal Behaviour Order (CBO) or acceptable behaviour contract (ABC).

This list is not exclusive and partnerships must ensure that target criminals reflect local concerns and priorities and are also consistent with the Data Protection Principles.

'In or near' the operational area will generally mean the administrative district or borough within which the partnership is established.

Data Disclosure

Data shall not be disclosed to any non-member, unless required to do so by the law or by the order of a ruling of a court, tribunal or regulatory body. If required to do so, the member should notify the crime manager promptly, prior to making such disclosure.

Data Security

Appropriate security measures will be taken to ensure that personal data is kept securely in accordance with the Partnership Protocols. Members must prevent unauthorised access to, or alteration, disclosure, accidental loss or destruction of personal data. This may constitute a breach of the Data Protection Act and may lead to further action.

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Target files, photographs or other personal data will be returned to the crime manager or securely destroyed when requested to do.

Target files and other information will be transmitted to authorised persons only through secure channels.

In consideration of personal data being made available, the member undertakes the following:

1. To keep the data confidential at all times.
2. To obtain and process data and information fairly and lawfully.
3. To collate the data solely for the purposes of prevention and detection of crime, or the apprehension or prosecution of offenders.

DATA INTEGRITY AND MEMBERSHIP AGREEMENT

I confirm that I understand the responsibilities relating to the management of personal data about living persons contained in the Data Integrity Statement. I undertake to ensure that any information to which I or members of my company/ organisation have access to will be managed according to the 6 Principles of Data Protection and any partnership documentation and protocols which may pertain.

I understand that any breach of this agreement may be dealt with in accordance with the disciplinary procedures of the partnership. Making an unauthorised disclosure of data may lead to criminal prosecution.

I have received a copy of the Data Integrity Statement and partnership documentation and protocols. I understand the contents and agree to operate within their conditions, policies and procedures.

NAME:

SIGNATURE:
(For and on behalf of the member)

COMPANY/ORGANISATION.....

POSITION:

ADDRESS:
.....

EMAIL
.....

Telephone

DATE:

NAME:

SIGNATURE: (For and on behalf
of the partnership)

DATE: