North Notts Business Crime Reduction Partnership

Code of Practice

Operating Guidelines

February 2021

Section 1

CODE OF PRACTICE

Contents

Introduction 3
The AIm 3
Description of Partnership 3
Statement of Purpose 3
Partnership Discipline 4
Training 4
Employees 4
Third Party Employees 4
Disclosure of Information 5
Security/Audit 5
Indemnity Insurance 6
Media Relations 6
Data Protection Principles 6
Data Protection Requirements 6
Subject Access 7
Complaints 8
Links to other Partnerships 8

Section 1

Code of Practice

1. Introduction

1.1 This Code of Practice is to control the management, operation, compliance and use of the data and service of the NNBCRP.

1.2 This document has been prepared following advice from the Information Commissioner, the Police and other contributors to the legal process. It operates strictly within the provisions of the Data Protection Act 2018.

1.3 The document will be subject to periodic review following consultation with all interested Parties, to ensure it continues to reflect its stated purpose and remains in the public and participants interests.

2. The Aim

2.1 To lawfully and legitimately gather, collate, exchange, process and manage all information relating to crime, its commission and perpetrators by members of the NNBCRP, to reduce and prevent criminality and anti-social behaviour, in order to create a safe and secure environment within.

3. Description of the Partnership

3.1 NNBCRP is an information sharing and support network between the business community, police and other crime preventions agencies in the Bassetlaw area.

NNBCRP aims to assist in detecting and deterring crime through local information gathering and sharing in line with the Data Protection Act 2018. As a local partnership, NNBCRP has an obligation to liaise with external partnerships and organisations, exchanging relevant data where Information Sharing Agreements exist in furtherance of the stated aims. To reduce crime and disorder.

4. Statement of Purpose

4.1 The NNBCRP will be operated fairly and in compliance with current legislation only for the stated aim and objective for which it was established.

4.2 Each member, participant and contributor of NNBCRP is and remains bound by this Code of Practice and any subsequent amendments to it,

4.3 All persons considered for such employment must demonstrate an adequate knowledge of all the relevant legislation including the Data Protection Act and in addition any other relevant legislation to the partnership.

5. Partnership Discipline

5.1 NNBCRP has specific responsibilities, which must be understood by all members and their representatives. Each member must sign a Member Agreement, which incorporates the NNBCRP Data Sharing Policy which will be strictly adhered to by the data controller, employees of the partnership and members. Non-compliance of the Data Protection Act 2018 may lead to criminal prosecution and/or civil actions for damages. Lesser infringements of procedure may be subject to sanction by the Management Committee. This may be in the form of training, verbal and written warnings or removal from the partnership.

6. Training

6.1 In order to maintain high standards NNBCRP will establish and maintain a training programme for managers, employees and agents of participating businesses. The purpose of the training is to ensure that all concerned are fully aware of the procedures applicable to the initiative and of their personal roles and responsibilities.

6.2 A nominated NNBCRP contact within each business outlet will liaise with the NNBCRP appointed staff as and when new employees are introduced to the NNBCRP service. New members of staff will undergo appropriate training to ensure they are aware of their responsibilities.

7. Employees

7.1 Numbers of staff employed by NNBCRP will be determined by the Steering Group to meet the business requirements of the Partnership.

7.2 Matters relating to the employees welfare, safety at work, performance/appraisal, general conditions of employment and working relationships will be the responsibility of the NNBCRP Steering Group in compliance with existing policy documents.

7.3 The day to day running of the Partnership will be carried out by the appointed NNBCRP Steering Group who will report to the NNB Board as necessary.

7.4 In order to maintain high standards NNBCRP will establish and maintain a training programme for employees. The purpose of the training is to ensure that all concerned are fully aware of the responsibilities in relation to data management, procedures applicable to the initiative and of their personal roles and responsibilities.

7.5 Employees will be required to disclose previous convictions on recruitment and throughout their employment.

8. Third Party Employees

8.1 Participating businesses may be represented by third party organisations such as guarding, store detectives or other out-sourced security services.

8.2 Disclosure of NNBCRP data to such employees must only be provided for under the Data Protection Act 2018 and only following assessment by the data controller. The decision to disclose will

necessarily have to be on a case-by-case basis and should not be regarded as being available under an automatic authority.

8.3 The Management Committee will retain the power of veto on individual third party organisations in the appropriate circumstances.

8.4 Third party staff, who are employed by Partnership members, must abide by the same codes of practice/operating guidelines/data protection agreement which forms the structure of the Partnership.

9. Disclosure of Information

9.1 The information and intelligence held within the NNBCRP office is confidential. No disclosure of information will take place that is not in accordance with the relevant statutory provisions. The data held may only be accessed and shared by Partnership members after signing the appropriate documentation.

9.2 The NNBCRP must be notified to the Information Commissioner as required under the Data Protection Act 2018 identifying the NNBCRP Manager as the main contact and the NNBCRP Management Committee as Data Controller.

9.3 Further information in relation to the constraints on the use of information please see NBCS050, Data Sharing Policy section 6.

10. Security/Audit

10.1 All information received from participants will be assessed in terms of its intelligence value and will, if found to be of value, be held on the NNBCRP database, in accordance with the guidelines of the National Intelligence Model.

10.2 The Partnership will maintain appropriate levels of security, in accordance with good practice and the requirements of legislation

10.3 Members will maintain like standards of security in respect of all information in their custody.

10.4 Each member agrees to appoint a locally designated representative to assume responsibility, for the protection and security of data disclosed and exchanged in the partnership, for ensuring that all security rules are applied and to facilitate any audits. However, the overall responsibility for the Partnership's compliance with the Data Protection Act 2018 lies with the members' data controller.

10.5 NNBCRP and members will submit to inspections when required with a detailed audit report against the requirements and principles of Data Protection Act 2018 and Code of Practice. The results will be made available.

10.6 If members fail to comply with the NNBCRP's Code of Practice, a written letter explaining why will be written to the member to rectify the situation. Any further failure will result in withdrawal of the NNBCRP service with a written report submitted to their Head Office, where applicable.

11. Indemnity Insurance

11.1 NNBCRP must provide appropriate insurance cover for employees and officers of the Partnership.

11.2 Members of the Partnership should ensure that adequate insurance exists within their own organisations.

12. Media Relations

12.1 All media enquiries should be referred to the NNBCRP Manager in accordance with the NNBCRP policy who will decide upon an appropriate response. Individual Members should not seek to represent the Partnership without consultation.

13. Data Protection Principles

13.1 All relevant details relating to the lawful basis NNBCRP will share information can be found in the NNBCRP's Data Privacy Impact Assessment NBCS0052.

13.2 All members and their representatives of the Partnership should not only be aware of these principles but also have a good working knowledge of the Act. This is particularly important for data controllers and processors who must not rely purely on these principles.

14. Data Protection Requirements

14.1 All staff who have access to personal Data recorded on the NNBCRP system must be made aware of and comply with the Data Protection Principles in article 5 of GDPR. These 7 principles include:

- **a)** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to Individuals
- **b)** Personal data shall be collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes.
- **c)** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **d)** 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.
- **e)** 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.
- **f)** 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.
- **g)** Article 5(2) adds that… "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')"

14.2 All staff allowed access to the NNBCRP data must sign a Data Protection Declaration through the crime management platform.

14.3 The Partnership procedures need to be monitored periodically to ensure efficient operation:

a) The Management Committee and/or any representatives authorised on their behalf will audit individual members a minimum of once a year to ensure security and confidentiality. A record will be kept by the Partnership manager or nominated person of the audit, e.g. date carried out and by whom.

b) Any shortcomings identified must be rectified.

14.4 Any changes to nominated contacts with individual members must be communicated immediately to the NNBCRP office.

14.5 NNBCRP will ensure that security measures are in place if transferring data electronically.

14.6 Where appropriate, NNBCRP data will be handled in accordance with current management of police information (MOPI) guidelines

15. Subject Access

Persons may request access to all and any of their person data processed by **NNBCRP** 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.

15.1 Complying to any Subject Access requests must be in accordance with the Data Protection Act 2018. Third party rights must be protected, and this responsibility lies with the NNBCRP data controller.

15.2 The NNBCRP data controller is not obliged to supply information unless he/she has received the request in writing and has confirmed identification of the person making the request and established that the person making the request is the data subject.

15.3 The NNBCRP data controller must comply with a request promptly, before the prescribed period. The Data Protection Act 2018 defines the prescribed period to within 40 days of receipt of the request.

15.4 Please contact NNBCRP if a Subject Access Request of NNBCRP information is received at your member premise.

16. Complaints

16.1 Complaints should be brought to the attention of the data controller. Any formal complaint by a data subject regarding any stage in the partnership process of their personal data should be notified in writing to the relevant partnership members only and a decision made as to who will lead in responding to the complaint given the specific circumstances.

17. Links to Other Partnerships

17.1 If NNBCRP shares data with other Partnerships, these Partnerships must comply with the requirements of current data protection legislation and have signed the NNBCRP Information Sharing Agreement.

Section 2

OPERATING GUIDELINES

Contents

Introduction……10

Membership Requirements……10

The Partnership Contact……10

Definition of a Target……11

Definition of an Incident……11

Data Accuracy……13

Creation of the Intelligence Bulletin ……13

Use of partnership Information……13

Ownership and Rights of use of Images……13

Communication……13

CCTV Evidence……13

Arrest Procedures……14

Data Input/Analysis Procedure……14

Storage of Data……14

Input of Data……14

Rationalisation of Files……14

Target Tracking……14

Management Information……15

Additional Security……15

Section 3

OPERATING GUIDELINES

1. Introduction

1.1 The aim of this Operating Guide is to provide a set of working procedures for members of the NNBCRP. It will be reviewed and updated as and when necessary following consultation.

1.2 NNBCRP will be based at the following postal address:

North Notts BID Ltd
West Retford Hall
Rectory Road
Retford
DN22 7AY

2. Membership Requirements

2.1 Membership of NNBCRP will require acceptance and signature of the Membership Agreement, Codes of Practice and Data Sharing Policy and in cases of external partnerships information sharing agreements.

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

a) to keep all information received through the NNBCRP confidential and, save as otherwise permitted, 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;
b) not to print any Personal Data from the NNBCRP's website/App;
c) not to copy any Personal Data from the NNBCRP's website/App into any other system;
d) to submit Incident Reports on persons by using the secure online facilities available through the NNBCRP's Website/App;
e) to ensure that information on the NNBCRP 's Website/App is only accessed by or disclosed to other Members of the NNBCRP;
f) to ensure that appropriate security measures are employed to prevent unauthorised access to, or alteration, disclosure or destruction of Personal Data provided through the NNBCRP Website/App;
g) to allow the NNBCRP to audit each Member's compliance with the above obligations;
h) to ensure that, where relevant, the Member's employer organisation is compliant with current Data Protection law including registration with the Information Commissioner's Office and

designation of an internal Data Controller.

3. The NNBCRP Contact

Each member premise must have a named contact to enable NNBCRP to send information to and contact for other purposes. All hard copy information will be sent to the nominated NNBCRP contact. All NNBCRP contacts must complete the New Member Account Details form NBCS0047. The NNBCRP contact will be responsible for ensuring the service is delivered with the member business, appropriate staff are trained to use the NNBCRP service and systems and to notify the partnership of any changes to personal as is relevant to the service.

4. Definition of a Target

The NNBCRP may display names and/or images of 'Targeted Persons' on the NNBCRP 's Website/App. These persons have either been subject to a single Incident Report for criminal or anti-social behaviour by Members or their personal information has been supplied to the NNBCRP 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 NNBCRP Website is to:

- ensure that such persons are aware that the NNBCRP knows their identity, and thus to encourage them to desist in any further criminal or anti-social behavior in the NNBCRP 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* NNBCRP Exclusion Policy) his/her Personal Data will be withdrawn from display on the NNBCRP Website/App after 6 months. This data will continue to be accessible in the crime management database only to the NNBCRP's Administrator and nominated Members with full Administrator rights subject to the NNBCRP's policy on Irrevocable Erasure of Personal Data.

5. Definition of an Incident

5.1 Incidents to be Reported:

a) Any crime or attempted crime against any member that falls within the scope of the partnership remit. This may be offending within Bassetlaw area.

b) Sightings of person(s) known or believed to be involved in offending behaviour.

c) Any new associates of person(s) known or believed to be involved in offending behaviour.

d) Any vehicles linked to the above.

e) Any other relevant and appropriate information from within or near the area of operation as defined by the partnership.

Incident Reporting

All members are encouraged to report Incidents to the partnership in order to build the database, increase knowledge and be able to respond timely and effectively of any possible threat. Members can submit a report either through the NNBCRP crime reporting platform or via secure email.

To avoid the scheme being brought into dispute, all information and reports submitted to NNBCRP *must be accurate and relevant. Any image submitted should leave no doubt about whom the subject is. Reports should be completed during or as soon as possible after the incident while everything remains clear in your mind.*

The following incidents are a guide to help encourage reporting to the partnership:

Theft and Attempted Theft

Person(s) arrested for theft or attempted theft:

a) Incidents where the thief escapes with merchandise without being apprehended.
b) Person(s) involved in theft where property is subsequently abandoned in or outside the business premises.

Deception

Where a theft takes place and an offender obtains or attempts to

a) obtain a refund or exchange on those goods.
b) Where the price of goods has been altered to reflect a lower price
c) The use of a counterfeit receipt to obtain a refund on stolen property
d) Counterfeit money used for the purchase of goods

Criminal Damage/Attempted Criminal Damage

Where a person is involved in causing or attempting to cause damage to goods, property or buildings.

Street Crime

Person(s) involved in pick pocketing, bag theft, robbery, violence, anti-social behaviour and disorder within the partnership area. These offences may take place inside or outside members' premises.

Sightings

Of person(s) known or believed to be involved in crime. They may not commit an offence but may be acting suspiciously.

Assaults or Insulting or Threatening Behaviour

Where an offender:

a) Physically assaults a member of the public or staff
b) Verbally threatens a member of the public or staff
c) Intimidates a member of the public or staff.

Breach of an Exclusion Notice

Where an offender has previously been served with a partnership exclusion notice, court order or store ban.

Breach of an Anti-Social Behaviour Order (ASBO) or Acceptable.

Behaviour contract (ABC), or such similar orders as are introduced.

Breach of Bail Conditions.

Any other appropriate incident affecting your business or local area.

6. Data Accuracy

6.1 Incident details will be audited to ensure that all information remains current and accurate in order to satisfy the requirements of Data Protection Act 2018 and the General Data Protection Regulation. Data will be monitored and screened according to the National Intelligence Model Guidelines.

7. Creation of the Intelligence Circulation

7.1 The NNBCRP appointed staff will prioritise and focus on the most prolific current business offenders and other criminals. This file will be updated and circulated accordingly.

8. Use of NNBCRP Information

8.1 NNBCRP information must only be used for the purpose of preventing and detecting crime.

NNBCRP information must be treated as restricted by members and only be viewed by management, CCTV operators, store detectives, guards and other authorised staff who have signed the appropriate documentation.

NNBCRP information is for reference only and not for public or private display.

9. Ownership and rights of use of images

When a Member submits an image of a person to the **NNBCRP** either through the Website/App or through any other method, the Member grants the **NNBCRP** 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 **NNBCRP**.

In the case of unidentified images of persons, the submitting Member grants the **NNBCRP** unlimited rights to share the image with other Business Crime Reduction Partnerships and authorised third parties for identifying the person displayed.

10. Communication

10.1 A regularly updated member contact list must be maintained by the NNBCRP appointed staff. It is the responsibility of each member to provide this information.

11. CCTV Evidence

11.1 CCTV footage should be retained in compliance with the Data Protection Act 2018 and Code of Practice and the disclosure rules. In the effort to identify suspected business offenders the NNBCRP will produce a still from footage provided. The production of the still will be classed as Data.

12. Arrest Procedures

12.1 If the target commits an offence and is arrested, he/she should be processed in accordance with the normal company procedures and the police contacted. In the case where the offender is a target this information should be indicated to the attending police officer.

13. Data Input/Analysis Procedures

13.1 ***Data Definitions***

Data means information in a form that can be processed.
Data Equipment means equipment for processing.
Data Material means any document or other material used in connection with, or produced by, data equipment.

Disclosure, in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data (but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties;) and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall not be regarded as disclosed unless the other information is also disclosed.

14. Storage of Data

14.1 All data/information received by the NNBCRP will be stored on the NNBCRP database in a secure location. Access to said data/information would be logged in accordance with procedures. The access and management of data applies to both electronically held and manual data.

15. Input of Data

15.1 The NNBCRP appointed staff and anyone authorised by the Management Committee will have sole responsibility for the input all data onto the NNBCRP database. All data entries will be quality assured in accordance with the Data Protection Act 2018, the General Data Protection Regulation and National Intelligence Model guidance.

16. Rationalisation of Files

16.1 If a target has not been active within the agreed period (see Section 9 – NBCS0050 Data Sharing Policy), data in respect of him/her will be removed to a dormant file for a further limited period

before deletion/destruction. This will not apply where a person is known to have been in prison or abroad over the relevant period.

17. Target Tracking

17.1 A major part of the Partnership is to use intelligence-driven pro-activity against persons who engage in business and associated crime on an organised basis. An additional component will be the tracking of persons as they move through the criminal justice system.

18. Management Information

18.1 It will be necessary to establish key performance indicators (KPIs) to measure the operating success of the partnership and provide management information if required.

18.2 The partnership is a key facility to improve the gathering, sharing and collation of information about crime and anti-social behaviour and each member and partner agency has an obligation to provide information, as appropriate, to enable this important activity to happen.

18.3 One of the important functions in the set-up of the Partnership will be to clearly identify what management information is required, the frequency it will be produced, and in what format.

19. Additional Security

19.1 Procedures will be in place to ensure full compliance with data protection and other legal obligations. These include: -

a) **Visitors Log**. Access to the NNBCRP office will be controlled and all visitors will be logged in and out. All visitors must sign on entry to the office acknowledging their acceptance of confidentiality of data and the reason for their visit.

b) **Technical security:** All personal data will be processed within the DISC; the security provisions of the DISC are described in the document Rules and Protocol ; Members can access the NNBCRP data only through the DISC desktop or App.

c) **Organisational security**: where it is necessary for personal data to be stored temporarily outside the DISC system, the NNBCRP 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.