Derbyshire Constabulary

INFORMATION SHARING AGREEMENT

CRIME & DISORDER
(Safer Derbyshire Research and Intelligence)

Document owner	**Chief Superintendent Gary Knighton**
Document author and enquiry point	**Nicola Henshaw, Performance Manager**
Document authoriser	**Abby Turner, Head of Information Management**
Review date of document	**07/11/2013**
Version	**1.0**
Document classification	**Not Protectively Marked**
Document distribution	**Listed partners**
Document retention period	**Until date of next review**
Next document review date	**May 2014**

Date issued	Version	Status	Reason for change
07/11/2013	1.0	Final	First Issue

Introduction

The Crime and Disorder Act (1998) outlines the need for Responsible Authorities to share information in order to reduce instances of crime and anti-social behaviour in their local area and the Crime and Disorder (Prescribed Information) Regulations 2007 outlines the types and extent of information to be shared under the Act.

This information sharing agreement formalises the nature of data sharing between Derbyshire Constabulary, Derby City Council Research and Intelligence Team, Derbyshire County Council and the Safer Derbyshire Research and Intelligence Unit (SDRI) and under this Act.

This Information Sharing Agreement has been developed under the overarching principles of the Derbyshire Partnership Forum Joint Information Sharing Protocol and replaces any former agreements by the parties named for the described purpose(s).

1. Partners, and Partner Responsibilities

1.1 Partners

1.1.1 The partners to this agreement are as follows:

Derby City Council – Research and Intelligence Team
Derbyshire County Council – Safer Derbyshire Research and Intelligence Unit
Derbyshire Constabulary

1.2 Responsibilities

1.2.1 It will be the responsibility of each signatory to ensure that:

- realistic expectations prevail from the outset;
- designated points of contact (designated managers) are identified;
- a mechanism exists by which the flow of information can be controlled;
- the agreement, its purpose and objectives are communicated to all relevant staff;
- adequate arrangements exist to test adherence to this agreement and that data protection and other relevant legislative requirements are met.

2. Purpose and Objectives

2.1 As part of the Crime and Disorder Act, Responsible Authorities are required to work in partnership to do all they "reasonably can to prevent crime and disorder" (S17). Section 17A of the Act outlines the need to share specific information between responsible authorities for this purpose.

2.2 The information shared is to be used for a research, history and statistics purpose in order to inform strategy development and local activity to reduce crime and disorder in the prescribed area.

3. Information to be shared

3.1 The information to be shared is outlined in regulation 2 of The Crime and Disorder (Prescribed Information) Regulations 2007. For the purposes of this agreement, sections 1 and 2 of the schedule apply which are:

1. Information held by the police force for the area on the category of each –

(a) anti-social behaviour incident
(b) transport incident
(c) public safety/welfare incident

in the area, as defined in accordance with the National Incident Category List in the National Standards for Incident Recording Instructions for Police Forces in England and Wales for 2007/08 and the time, date and location for each of these incidents

2. Information held by the police force for the area on the sub-category of each crime classified as –

(a) burglary
(b) criminal damage
(c) drug offences
(d) fraud and forgery
(e) robbery
(f) sexual offences
(g) theft and handling stolen goods
(h) violence against the person
(i) other offences

in the area, as defined in accordance with the Home Office Notifiable Offences List as at the date of the 2007 Regulations, and the date, time and location of each of those crimes.

3.2 Further identification of specific crime types such as Hate Crime will be identified by markers or flags against the relevant crime data.

3.3 The disclosure of information in this context constitutes 'personal data' and 'sensitive personal data' under the provisions of the Data Protection Act 1998 as defined at Appendix A.

3.4 The prescribed data will be sent on a quarterly basis from Derbyshire County Council – Safer Derbyshire Research and Intelligence Unit to Derby City Council – Research and Intelligence Team via approved secure means.

4. Basis for Information sharing – fair and lawful processing

4.1 The information exchanged within this information sharing agreement must:

- have lawful authority
- be necessary
- be proportionate

4.2 Lawful Authority

4.2.1 Each partner (or body acting on behalf of such partner) sharing information must have a specific legal duty or power to do so. Each partner will need to have a clear understanding of the legal basis which all other partners are operating.

4.2.2 Personal data must be processed fairly and lawfully and in particular, shall not be processed unless:

a) at least one of the conditions in schedule 2 (of the act) is met **and**

b) for sensitive personal data one of the conditions in schedule 3 is also met.

The partners to this agreement will meet the requirements of Schedule 2 of the Data
Protection Act 1998, for the processing of personal data by virtue of subsections 5b as follows:

5b) for the exercise of any functions conferred on any person by or under any enactment.

In the case of sensitive personal data, the partners to this agreement also meet a Schedule 3 condition by virtue of subsections 7b as follows:

7b) for the exercise of any functions conferred on any person by or under an enactment.

The relevant enactments are detailed at 4.2.3 and 4.2.4 below.

4.2.3 Section 17 of the Crime and Disorder Act 1998

Without prejudice to any other obligation imposed on it, it shall be the duty of each authority to which this section applies to exercise its various functions with due regard to the likely effect of the exercise of those functions on and the need to do all that is reasonably can to prevent, crime and disorder in its area.

4.2.4 Section 115 of the Crime and Disorder Act 1998

The Police have a common law duty to prevent and detect crime and a corresponding power to disclose information where necessary for the prevention or detection of crime. In exercising this power, they must act fairly, having regard to the circumstances of the case, and bearing in mind that such disclosure is the exception to the general principle of confidentiality. They should also bear in mind that both the public and the Government expect them to use their powers and their knowledge to prevent crime and reduce crime and disorder.

Section 115 Crime and Disorder Act provides that any person can lawfully disclose information where necessary or expedient for the purposes of any provision of the Act, to a chief officer of police, a police authority, local authorities, probation service or health authority, even if they do not otherwise have this power. This power also covers disclosure to people acting on behalf of any of the above named bodies.

4.3 Necessity

4.3.1 The information will only be exchanged where necessary for the purpose of analysing crime and disorder within Derbyshire.

4.4 Proportionality

4.4.1 To justify the proportionality of information shared it must be shown that:

- the assessing and managing of the risks posed by crime and disorder and the identification of appropriate actions to deal with it could not be effectively achieved other than by sharing the information in question;
- the disclosure of the information is a proportionate response to the need to protect a person or persons or community.

5. Terms of use of the information

5.1 Information shall only be obtained for the purposes detailed in this Agreement

5.2 It is acknowledged that data matching exercise will be required for the purposes of this agreement; however, partners will takes such steps as necessary to ensure that such exercises do not indentify individuals and that the data shall not be processed to support measures or decisions with respect to particular individuals.

5.3 The data shall not be processed in such a way that damage or distress is, or is likely to be, caused to any data subject.

5.4 The results of the research or any resulting statistics will not be made available in a form which identifies any data subject.

5.5 It is acknowledged that the results of the research, or statistics, may be disclosed to parties other than those party to this Agreement and such results or statistics may be published in the public domain.

5.6 Partners undertake to acknowledge the standards contained within the Anonymisation: managing data protection risk code of practice published by the Information Commissioner.

6. Information Quality

6.1. Information shared under this Agreement must be fit for purpose, which means that it must be adequate, relevant and not contain excessive detail which is beyond that required for the agreed purpose. Partners will keep appropriate records of the sources of information to provide for this.

6.2 Information discovered to be inaccurate, out-of-date or inadequate for the purposes detailed in section three should be notified to the original partner who has provided the information, who will be responsible for correcting the data and notifying all other recipients of the information who must make sure the correction is made.

6.3 Partners will ensure that there is an effective management regime to monitor data quality.

7 Information Retention, Review and Disposal

7.1 Data which are processed only in accordance with the terms of the Anonymisation Code of Practice may, notwithstanding the fifth data protection principle, be kept indefinitely.

7.2 It is intended that three years of data will be held at any one time on a rolling basis.

7.3 Each partner shall maintain an auditable record of all information disclosed.

8. Information Security

8.1. Each Data Controller has obligations relating to the security of data in his control under The Data Protection Act 1998.

8.2 The Partners to this agreement acknowledge the security requirements of the Data Protection Act 1998 applicable to the processing of the information subject to this agreement.

8.3 Each Partner will ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8.4 In particular, each Partner shall ensure that measures are in place to do everything reasonable to:

- make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport;
- deter deliberate compromise or opportunist attack;
- dispose of or destroy the data in a manner to make reconstruction unlikely;
- promote discretion in order to avoid unauthorised access.

8.5 Access to information subject to this agreement will only be granted to those professionals who 'need to know' in order to effectively discharge their duties.

8.6 Any suspected breach or threat to the security of the information will be reported to all relevant Parties, via the relevant senior investigating officer without delay.

8.7 It is acknowledged that the Government Protective Marking Scheme applies to Police information.

8.8 Partners undertake to ensure that all of their staff are aware of their obligation to maintain the confidentiality of information provided by the Police and not to disclose information further. As such all relevant staff and agencies will adopt the Government Protect Marking Scheme for information shared under this agreement, or another approved protective marking scheme of an equivalent standard.

8.9 Information should not be disclosed to any persons who are not partners identified within this agreement, or if there are any doubts that the conditions set out in this agreement have not been met, or may be breached.

8.10 Information will normally only be transferred electronically via Egress Secure Storage Solution. Partners should check with designated Information Security staff for advice.

8.11 In cases where information is being exchanged by telephone, the person giving the information will always confirm the identity of the person receiving the information by making the phone call via a partner switchboard.

9. Management of the Agreement

9.1 Individual Rights to Access Information

9.1.1 Any person receiving a request for information under the provisions of the Data Protection Act 1998 or Freedom of Information Act 2000 must refer the request to the relevant officer within their respective organisation in accordance with local policy and procedures and without delay.

9.1.2 Where a request for information includes that information provided by a partner organisation, the originating organisation will be informed in accordance with normal protocols. However, each organisation is responsible for their compliance with the Freedom of Information Act 2000.

9.1.3 Personal data which are processed only in accordance with the terms of this agreement are exempt from the provisions of section 7 of the Data Protection Act 1998 and consequently the rights of access to information afforded to individuals under that section do not apply.

9.2 Complaints Procedure

9.2.1 All complaints and breaches relative to this Agreement should be referred to the signatory of the relevant organisation who will take appropriate action.

9.2.2 All complaints or breaches relative to this agreement will be notified to the designated Data Protection Manager of the relevant organisation in accordance with their respective policy and procedures.

9.2.3 Complaints from data subjects will be investigated first by the Partner receiving the complaint. Actions which affect other Partners will not be taken without the consent of all Partners to this agreement.

9.2.4 The signatories will give all reasonable assistance as is necessary to the relevant Data Controller to enable him to:

- respond to an Information Notice served by the Information Commissioner;
- respond to complaints from the data subject;
- investigate any breach of the agreement.

9.2.5 Lead Officers or signatories will make sure that in the event of:

- security incidents involving case file data shall be subject of a review by the relevant partner agency in accordance with their own processes and procedures.

- any breach of this agreement, the Data Protection Manager is informed and the cases are reviewed in light of the circumstances of the breach.

- in case of an internal disciplinary matter, the Data Protection Managers will review procedures in view of the circumstances coming to light from the disciplinary matter.

- in the case of an equipment malfunction the lead officer will inform the signatories and will arrange an alternative form of exchange until repair.

9.3 Indemnity

9.3.1 Each Partner to this agreement will undertake to indemnify the other against any legal action arising from any breach of this Agreement by any person working for or on behalf of its own organisation.

9.4 Review and termination of the agreement

9.4.1 This agreement will be reviewed no later than six months after acceptance by all partners and then every 18 months thereafter.

9.4.2 Any Party to this agreement may at any time in writing terminate the agreement if any Party is in material breach of any obligation under the agreement.

9.4.3 Written notice should be provided by either Party regarding the termination of the agreement.

9.4.4 A Partner may suspend these arrangements in order to investigate and resolve any serious breach of this agreement.

9.4.5 Any such action will be notified in writing to the other Partners with immediate effect.

9.4.6 Partners will make every effort to resolve any dispute affecting the ability to share information under this agreement within 10 working days.

Appendix A Definitions

Personal Data

Data which relates to a living individual who can be identified;

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive Personal Data

Sensitive Personal Data means personal data consisting of;

a) racial or ethnic origin of the data subject

b) political opinions

c) religious beliefs of other similar beliefs

d) trade union membership

e) physical or mental health

f) sexual life

g) commission of alleged commission of offences

h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings of the sentence of any court in such proceedings.