

Waltham Forest's Community Safety Partnership



Data Exchange Protocol

March 2016

PREFACE

SafetyNet partners bear a collective responsibility to bring about reduced crime, disorder, substance misuse and behaviour adverse to the environment in Waltham Forest. An important principle of working collectively is the sharing of relevant information with partners that can help local residents, victims of crime, people with drug problems and offenders we work with as well as increase the impact of the interventions we are delivering. With the right safeguards in place it is possible for information sharing to take place in a way that helps deliver the better services that we all want, while still respecting people's legitimate expectations about the privacy and confidentiality of their personal information.

This Protocol has been revised in the light of the Crime and Disorder Reduction Partnership Reform Programme initiated by the Home Office in 2006. The aim of this revision is to support improved effectiveness of SafetyNet and the delivery in Waltham Forest of reductions in crime, disorder, substance misuse and behaviour adverse to the environment.

Only partners to this protocol may receive information within this framework. Prior to signing, officers with delegated authority should first read through this Data Exchange Protocol and if you have any questions prior to signing please contact Alison Smith (Alison.Smith@walthamforest.gov.uk).

Once you have agreed to the Protocol please sign and date the signature sheet (Appendix 1) and return this single sheet to:

Simon Bartlett
Rowan House
Cecil Road
Leytonstone
E11 3HF

1.0 Introduction

- 1.1 This protocol provides guidance on the principles of the partnership's data sharing arrangements, detailing what will be exchanged, by whom, with whom, for what purposes and with which safeguards in place to support strategic planning and help local partnerships to implement the provisions of the Crime and Disorder Act.
- 1.2 The protocol explains the principles that must be followed when exchanging information to obtain the following Orders: (This list is not exhaustive)
- Criminal Behaviour Orders
 - Acceptable Behaviour Contracts,
 - Sex Offender Orders,
 - Child Safety Orders,
 - Child Curfew Orders¹
 - Dispersal Orders
 - Closure Orders
 - Public Space Protection Orders
 - Civil Injunctions
- 1.3 The protocol applies to any exchange of information that supports action under any other provision of the Crime and Disorder Act. This includes an exchange of information to support legal proceedings under the Housing Act where such an initiative has been included within the local crime reduction strategy. This may be relevant to: (This list is not exhaustive)
- Drug Treatment and Testing Orders,
 - Community Orders with a Drug Rehabilitation Requirement,
 - Reparation orders,
 - Action plan orders,
 - Supervision Orders,
 - Detention and Training Orders,
 - Parenting Orders,
 - Multi Agency Public Protection Arrangements (MAPPA)
 - Integrated Offender Management (IOM) arrangements
 - Drug Intervention Programme (DIP) arrangements.
 - Multi agency risk assessment conferences (MARAC)
 - Anti Social Behaviour risk assessment conference (ASBRAC)

¹The principles will apply to any other Order created by the Act.

2.0 Context

2.1 Crime and Disorder Reduction Partnerships (CDRPs), created by the Crime and Disorder Act (CDA) 1998, are the vehicle for tackling crime, anti-social behaviour, behaviour that adversely affects the environment and substance misuse at a local level. CDRPs comprise local agencies whose level of involvement is stipulated in the section 5 of the CDA and these are known as Responsible Authorities, Co-operating Bodies or Invitees to Participate.

2.2 Responsible Authorities have a statutory duty to work with other local agencies and organisations to develop and implement strategies to tackle crime and disorder including anti-social behaviour and other behaviour adversely affecting the local environment as well as the misuse of drugs in their area². The Responsible Authorities are required to work in co-operation with a second layer of organisations to progress their statutory duty and invite a range of local private, voluntary and other public and community groups, including the public itself, to become involved in the needs assessment and strategy development process.

2.3 “Responsible Authorities” in any given local area in England comprise:

- Police
- Local Authority
- MOPAC
- Fire and Rescue Authority
- Local NHS services commissioned by Clinical Commissioning Group and NHS England
- Probation Trusts
- Registered Social Landlords

2.4 “Co-operating Bodies” are defined as

- NHS Trusts and NHS Foundation Trusts
- Governing bodies of schools and further education institutes
- Proprietors of independent schools
- Parish Councils

2.5 “Invitees to Participate” include:

- Voluntary Organisations
- Crown Prosecution Service
- Magistrates Court Committee
- Victim Support Scheme
- Transport for London

² s6, Crime and Disorder Act 1998 as amended by s97 and s98 Police Reform Act 2002 and s1, Clean Neighbourhoods and Environment Act 2005.

- British Transport Police
- 2.6 The Home Office initiated a review of the CDA in 2005 and this led subsequently to the development of the CDRP Reform Programme the purpose of which is to improve the effectiveness of local arrangements to tackle crime, anti-social behaviour, behaviour that adversely affects the environment and substance misuse.
- 2.7 The Police and Justice Act (PJA) 2006 took forward the proposals from the CDA Review and in August 2007, introduced some important changes to what is asked of CDRPS..
- 2.8 Schedule 9(4) of the PJA increases the scope of Section 17 of the CDA (the mainstreaming crime reduction requirement) to include anti-social behaviour, substance misuse and behaviour that adversely affects the environment.
- 2.9 Schedule 9(5) of the PJA strengthens the existing power to share information given by Section 115 of the CDA and introduces a new duty requiring partners to share depersonalised data, already held in a depersonalised format, for the purposes of reducing crime and disorder.

3.0 Definitions

For the purpose of this protocol:

“Crime” is defined as any act, default, or conduct prejudicial to the community the commission of which by law renders the person responsible liable to punishment by a fine, imprisonment, or other penalty.

“Disorder” refers to the level or pattern of anti-social behaviour within a particular area.

“Protocol” refers to this document and its appendices including any containing the signatures of contributing partners.

“Personal information” refers to data that relate to a living individual who can be identified either from the data, or from the data and any other information, which is in the possession of, or is likely to come into the possession of the data holder.

“Depersonalised information” refers to data from which it is no longer possible to identify an individual.

4.0 Guiding Principles

4.1 General

For Review: March 2017

- 4.1.1 Signatories to this protocol will abide by the eight key principles of the Data Protection Act (DPA) 1998. See APPENDIX 1 for details.
- 4.1.2 It is the responsibility of individual agencies to ensure that they notify the Information Commissioner of the type of personal information that they intend to process in support of this protocol.
- 4.1.3 All statutory provisions must be used in a manner that is compatible with the requirements of the Data Protection Act and the Human Rights Act and, unless the statutory provision clearly authorises disclosure, with the common law duty of confidentiality.
- 4.1.4 Any request involving the exchange of personalised data will be
- Made in writing
 - Made in a prescribed format and using the agreed SafetyNet template - Form 115 (see APPENDIX 2)
- 4.1.5 All requests involving the recurring exchange of de-personalised information will be also be:
- Made in writing
 - Made in a prescribed format and using the agreed SafetyNet template – Form 115 (see APPENDIX 2)
- 4.1.6 Ad hoc requests to exchange de-personalised information will be:
- Made in writing
 - Made in a prescribed format and using the agreed SafetyNet template – Form 115 (see APPENDIX 2).
- 4.1.7 All signatory agencies are deemed to be ‘relevant authorities’ in accordance with s115 of the Crime and Disorder Act.
- 4.1.8 This protocol will be subject to annual reviews.

4.2 Data Ownership

- 4.2.1 An underlying principle of the protocol is that an agency will always retain ownership of the personal information it discloses to another member of the partnership. A recipient of such information must therefore obtain the consent of the original

data owner before making a further disclosure³. For the purposes of this requirement each local authority department will be treated as a separate agency.

- 4.2.2 Where an agency receives a subject access application and personal data is identified as belonging to another agency, it is the responsibility of the receiving agency to contact the data owner to determine whether the latter wishes to claim an exemption under the provisions of the DPA.

4.3 Data labelling

- 4.3.1 There is a requirement that the accuracy and precision of depersonalised data must be defined before it is made available to other members of the partnership⁴.

4.4 Dealing with the media

- 4.4.1 The partners to this protocol subscribe to the following principles when discussing with the media issues that arise from the sharing of personal or depersonalised information:
- any information provided to the media is accurate, honest and fair;
 - information will not be divulged without the consent of the lead Policy Officer to the SafetyNet Executive or nominated individual;
 - each organisation in its dealings with the media will respect the professionalism and integrity of its partners;
 - Where there are differences of opinion between organisations these will not be commented on publicly without prior notice and discussion.
- 4.4.2 Press and public relations staff in each organisation should have a working knowledge of the structure, key issues and staff in other partner organisations. Opportunities for the placement of articles in the public media e.g. on partner web-sites/intranet pages and other publications should be encouraged.

5.0 What data will be shared

³ For this reason personal information stored on a YOT database must be cross-referenced to identify the original data owner.

⁴ The term precision refers to the geo-spatial level at which the data is presented: for example, postcode, ward or 250m grid. The level of accuracy refers to the percentage of the total available data that can be aggregated to the relevant level of precision.

- 5.1 This protocol covers both the exchange of personal information⁵, including sensitive personal information as defined by the DPA, and the release of depersonalised information.

6.0 By whom and with whom

- 6.1 Only those partners who are signatories to this protocol may exchange information within this framework.
- 6.2 The signatories to the protocol will nominate designated officers to process, or initiate requests for personal information⁶. A reply shall be made within ten working days.
- 6.3 Any person requesting information from another agency must submit the inquiry through a designated officer. When information is disclosed the recipient must ensure that it is stored securely and destroyed when it is no longer required for the purpose for which it was initially provided. If the information is requested electronically, then the person requesting the information must ensure that a secure e-mail address is provided for receiving the information.
- 6.4 A list of signatories appears at Appendix 3

7.0 Purposes of data exchange

7.1 Personalised Information

- 7.1.1 Section 115 of the Crime and Disorder Act enables the disclosure of personal information to be considered whenever it is necessary or expedient to the successful implementation of the Act.

7.2 Depersonalised Information

- 7.2.1 The exchange of depersonalised information should be considered where this could be used to:
- facilitate strategic planning;
 - identify areas of high crime or disorder, or substance misuse or anti-social behaviour;
 - measure the impact of CCTV or other preventative schemes;
 - Determine whether the local strategy to reduce crime, anti-social behaviour, behaviour adverse to the environment and substance misuse is delivering best value.

⁵ including conviction data

⁶ It is recommended that all requests should be made in writing

7.2.2 Schedule 9(5) of the Police and Justice Act 2006 introduces a new duty requiring relevant authorities to share depersonalised data. New regulations on data sharing are included at APPENDIX 4.

8.0 Safeguards

8.1 Personal Information

8.1.1 Although Section 115 of the Crime and Disorder Act enables the disclosure of personal information to be considered whenever it is necessary or expedient to the successful implementation of the Act, the provisions of the Human Rights Act and the Common Law presumption of confidentiality still apply. Grounds for processing personal data as defined by the Data Protection Act must also exist.

8.1.2 This means that in every case a designated officer must:

- identify why a disclosure is necessary to support action under the Crime and Disorder Act
- make an objective assessment of the facts to determine whether the public interest overrides the usual presumption of confidentiality and
- ensure that the information is being processed fairly

8.1.3 The grounds upon which a disclosure is based must then be recorded.

8.1.4 The personal details of a patient, victim, informant or a witness should only be disclosed with the explicit consent of the person concerned. In the case of a juvenile parental consent must also be obtained. It is recommended that consent be obtained in writing. Only where the public interest would be profoundly and adversely affected by a decision not to disclose should personal information of this nature be disclosed. Personal data is defined in the DPA (at section 1(1)), as “data which relate to a living individual who can be identified from those data; or 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”

8.1.5 Details of formal warnings and cautions, which relate to an adult, will not be disclosed as the cautioning procedure creates an

expectation that the offence has been dealt with and that no further action will be taken. The only exceptions will be:

- information released in connection with the vetting of applicants for local authority posts⁷; and
- Information provided to other agencies at risk management meetings to identify the potential threat posed by a sex offender.

8.1.6 The exchange of personal information post conviction is subject to the same presumption of confidentiality. However, the administration of justice and the prevention of crime are obviously in the public interest and will provide the grounds upon which a disclosure can be justified.

8.1.7 Any unauthorised access to or disclosure of information by an employee of a signatory agency will be treated as a serious matter and may be the subject of an inquiry. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents

8.2 Depersonalised Information

8.2.1 The following safeguards must be implemented in relation to depersonalised information exchange:

- maps and other visual images must not be published outside of the partnership without prior consultation with the original data owner(s);
- no attempt must be made to identify an individual through the provision of depersonalised information;
- data sets must not be released to those who have a commercial interest in their use;
- arrangements must be made for the secure storage of all depersonalised information in accordance with each agencies policies and procedures
- information must be destroyed when it is no longer required.

8.2.2 Any unauthorised access to or disclosure of information by an employee of a signatory agency will be treated as a serious matter and may be the subject of an inquiry. Each party will be accountable for any misuse of the information supplied to it and the consequences of such misuse by its employees, servants or agents

⁷ See Home Office circulars 22/91, 47/93, 42/94, 46/94.

APPENDIX ONE Legal Framework for Sharing Information

1.0 Sources of Law

- 1.1 The main sources of relevant law with respect to information sharing and confidentiality include: (this list is not exhaustive)
- Common law duty of confidence
 - Human Rights Act 1998
 - Data Protection Act 1998
 - Crime and Disorder Act 1998
 - Children Act 1989
 - The Caldicott Standards (applicable to health and Children's Social Services)
 - Children Act 2004
 - Housing Act 1996
 - Education Act 1996
 - NHS and Community Care Act 1990
 - Sex Offenders Act 1997
 - Freedom of Information Act 2000

2.0 Common Law

- 2.1 The 'Common Law Duty of Confidence' arises when a person shares information with another in circumstances where it is reasonable to expect that the information will be kept confidential e.g. a contract or a patient-doctor relationship.
- 2.2 The personal information about individuals, children and families kept by professionals and agencies should not generally be disclosed without the consent of the subject. Where there is a defined public interest in supplying the information, for example for the prevention and detection of crime, information can be disclosed without consent being sought.
- 2.3 The key factor in deciding whether or not to disclose confidential information is proportionality i.e. is the proposed disclosure a proportionate response to the need to protect the child's welfare. The amount of confidential information disclosed and the number of people to whom it is disclosed should be no more than is necessary

to meet the public interest in, say, protecting the health and well-being of the child.

- 2.4 The approach to confidential information should be the same whether any proposed disclosure is internally within an organisation or between agencies.

3.0 The European Convention on Human Rights

- 3.1 Article 8 of the Convention states that:

- Everyone has the right to respect for her/his private and family life, home and correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, protection of health or morals or for the protection of rights and freedom of others.

- 3.2 The right is not absolute and there are certain situations when Article 8 enables professionals to disclose information without consent e.g. to:

- Safeguard a child
- Protect her/his health or morals
- Protect the rights and freedoms of others or
- Prevent disorder or crime

- 3.3 Article 8 is only one of the articles of the Convention. The Convention also expressly enshrined the right of all citizens not to live in degrading or inhuman conditions for instance and children are citizens under the Act just as are adults.

- 3.4 As with the common law described above, the principle of 'proportionality' applies to sharing confidential information i.e. when disclosing information without consent one must limit the extent of the disclosure to that which is necessary to achieve the aim of disclosure i.e. to protect the child.

4.0 Data Protection Act 1998

- 4.1 The Data Protection Act 1998 regulates the handling of information kept about a living individual on a computer or in a manual filing system and requires that personal information comply with the eight data protection principles:

- Obtained and processed fairly and lawfully

- Processed for limited purposes and not in any manner incompatible with those purposes
- Adequate, relevant and not excessive
- Accurate and relevant
- Held for no longer than necessary
- Processed in accordance to individual rights
- Kept secure
- Not being transferred to countries outside the EU without adequate protection

4.2 Information can be shared when **at least one** of the legitimate conditions in Schedule 2 of the Data Protection Act 1998 for sharing information are satisfied, these include:

- The data subject has consented to the processing
- Disclosure is necessary to comply with a legal obligation
- It is necessary to protect the vital interests of the data subject
- It is necessary for the exercise of a statutory function or other public function exercised in the public interest e.g. a s.17 assessment or s.47 enquiry and
- It is necessary for the purposes of legitimate interests pursued by the person sharing the information (except where it is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the data subject)

4.3 If the information being shared is 'sensitive personal data' e.g. racial or ethnic origin, religious beliefs or political opinions, trade union membership, sexual life, criminal offences, one of the following additional conditions of Schedule 3 must be met:

- The subject has explicitly consented
- It is necessary to protect her/his vital interests or those of another person where the subject's consent cannot be given or is unreasonably withheld or cannot reasonably be expected to be obtained
- It is necessary to establish, exercise or defend legal rights
- It is necessary for the exercise of any statutory function and
- It is in the substantial public interest and necessary to prevent or detect an unlawful act and obtaining express consent would prejudice those purposes, for example the prevention and detection of crime.

4.4 More guidance on the Data Protection Act is available from the Information Commissioner's website: www.dataprotection.gov.uk

5.0 The Caldicott Standards

- 5.1 For NHS and councils with Children's Social Services responsibilities, the Caldicott principles and processes provide a framework of quality standards for the management of confidentiality and access to personal information under the leadership of a Caldicott Guardian.
- 5.2 Health and Children's Social Services must ensure that their information sharing arrangements are compliant with their own local procedures based on the Caldicott Standard (see *Health Service Circular/LAC circular HSC 2002/002/LAC (2002) 2 'Implementing the Caldicott Standard into Social Care'*).
- 5.3 Each health service and Children's Social Services will have their own Caldicott Guardian who should be able to provide advice and guidance as required.

6.0 Crime and Disorder Act 1998

- 6.1 The Crime and Disorder Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.
- 6.2 Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.
- 6.3 However, whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the data.

7.0 Overall Legal Position with Regard to Child Protection

- 7.1 All professionals have a duty to disclose information where failure to do so would result in a child or children or others suffering from neglect, or physical, sexual or emotional abuse.
- 7.2 In general, the law does not prevent individual sharing information with other practitioners to assist in safeguarding a child if:
 - Those likely to be affected consent *or*
 - The public interest in safeguarding the child's welfare overrides the need to keep the information confidential *or*
 - Disclosure is required under a court order or other legal obligation

Waltham Forest's Community Safety Partnership



Data Exchange Protocol

Organisation WFHA.....

Name ...Jo Joannou.....

Position/Title Housing services Manager
.....

Email Address joj@wfha.org.uk.....

Signature

.....
.....

Designated Information Sharing Liaison Officer (if different from above)

Name

E-mail Address

Contact Number ...0208524 6987.....

Date ...5/9/2016.....

Information Sharing Regulations

In each case, the duty applies to information relating to the partnership area as defined by the district or unitary authority area. This duty only applies when the authority holds the information so it does not require the collection of any additional information. The purpose of sharing this information is to enable the profiling or crime and disorder trends and patterns within the area. For this reason, in most cases, it is the record level data that is specified rather than aggregate data or statistics. Analysis can then take place across a number of different datasets on at least a quarterly basis.

Organisation	Datasets (for the area)
Police force	1. Records on anti-social behaviour, transport and public safety/ welfare incidents recording according to the National Incident Category List. Whatever information is recorded about the time, date, location and category of each incident must be disclosed. 2. Crime records recorded according to the Notifiable Offences list. Whatever information is recorded about the time, date, location and sub-category or each crime must be disclosed.
Fire and rescue authority	3. Records on deliberate fires, whether it was a deliberate fire (not a vehicle), a deliberate secondary fire (not in a vehicle) or a deliberate fire in a vehicle. In addition, records on incidents of violence against employees and records of fires attended in dwellings where no smoke alarm was fitted. For all these records, whatever information is recorded about the time, date and location of the fire must be shared. 4. Records on malicious false alarms. Whatever information is recorded about the time and date of each call and the purported locations of those alarms must be shared.
Local authority	5. Records on road traffic collisions. Whatever information is recorded about the time, date, location and the number of adults and children killed, seriously injured and slightly injured in each road traffic collision must be shared.

Organisation	Datasets (for the area)
Clinical Commissioning Group (lying entirely or partly in the area)	6. Records on fixed term and permanent school exclusions. Whatever information is held about the age and gender of the pupil, the name and address of the school from which they were excluded and the reasons for their exclusion must be shared. 7. Records of racial incidents. Whatever information is held about the time, date and location of each incident must be shared. 8. Records of anti-social behaviour incidents identified by the authority or reported to the public. Whatever information is held about the category, time, date and location of each incident must be shared. 9. Records on various categories of hospital admissions. The relevant admissions are those relating to the following blocks within the International Classification of Diseases: a) assault (X85-Y09); b) mental and behavioural disorders due to psychoactive substance use (F10-F19); c) toxic affect of alcohol (T51); and d) other entries where there is evidence of alcohol involvement determined by blood alcohol level (Y90) or evidence of alcohol involvement determined by level of intoxication (Y91). For each record, whatever information is held about the date of admission, the sub-category of the admission and the outward part of the postcode (the first part of the postcode, before the space which separates it from the second part) of the patient's address must be shared.

	10. Records of admissions to hospital in respect of domestic abuse . Whatever information is held about the date of the admission and the outward part of the postcode of the patients address must be shared.
--	---

Organisation	Datasets (for the area)
	11. Numbers of mental illness outpatient first attendances and persons receiving drug treatment. 12. Records of ambulance call outs to crime and disorder incidents. Whatever information is held about the category, time, date and locations of each ambulance call out must be shared.