Oxfordshire Safer Communities Partnership Information Sharing Protocol

For the purposes of exchanging

Community Safety

Information

Cara Langford
Oxfordshire County Council

The Oxfordshire Community Safety Information Sharing Protocol
Version 6 (08.06.15)

Table of Contents

Section 1

Guiding Principles

1. Purpose of this protocol

The purpose of this protocol is to facilitate the exchange of sensitive, personal and depersonalised information pursuant to the power contained in Section 115 of the Crime and Disorder Act 1998. It also meets the duties outlined in the Crime and Disorder Prescribed Descriptions Regulations 2007/1830 to have in place arrangements for the sharing of information between responsible authorities and a protocol setting out those arrangements.

The secure exchange of information to support the partnership working of the Community Safety Partnerships and to develop and implement a strategy and tactics for tackling crime, anti-social behaviour, substance misuse, youth offending and supporting victims in Oxfordshire.

This protocol has been ratified by the Oxfordshire Safer Communities Partnership, the strategic partnership tasked with coordinating community safety activities in Oxfordshire.

This protocol only covers community safety information and data sharing. It is noted that other information sharing protocols and agreements may be in situ with partner agencies to reflect other areas of work, for example, the Oxfordshire Children Safeguarding Board Information Sharing Protocol.

Section 1 describes the guiding principles for any information exchange under this protocol. These principles conform to the Data Protection Act 1998, Crime and Disorder Act 1998, and the Freedom of Information Act 2000, as well as guidance from the Information Commissioner's Office website.

Section 2 details the specific procedures involved in facilitating data exchange in Oxfordshire under this protocol. Central to this is identification of designated officers in each partner agency and the use of an information sharing schedule for each type of information exchange. The Oxfordshire Safer Communities Partnership is responsible for the protocol and will be central in ensuring compliance with this protocol.

Section 3 contains the appendices to this protocol including a copy of the information sharing schedule template.

Annexed documents as part of this protocol contain the signatories of this protocol and completed information sharing schedules. It is the intention of this protocol to include a broad range of signatories reflecting the strong community safety partnership relationships in Oxfordshire.

1.1 Why share information?

The use of good quality information and intelligence is essential in identifying and limiting the activities of those committing crime and disorder and in tackling those problems that adversely affect community safety and quality of life. It can also help to develop effective interventions at a much earlier stage to prevent those identified as being at risk from becoming offenders or victims. The more complete the picture of an individual's circumstances – not just contact with police or other community safety agencies, but also knowledge of support already provided by agencies, medical or social issues, family or life

stresses – the more informed and effective will be any intervention agreed and delivered.

Sharing information is fundamental to the success of any strategy to reduce crime and disorder, reduce the risk of terrorism and radicalisation, and to promote community safety and tackle substance misuse. It is vital that information exchanged between agencies working with those at risk of offending, and partners involved in securing legal orders such as Criminal Behaviour Orders, is done so with robust and secure systems and procedures.

The Crime and Disorder Act 1998, Police Reform Act 2002 and the Crime and Disorder (prescribed Information regulations) 2007 place an obligation on a variety of agencies to co-operate in the development and implementation of a strategy for tackling crime and disorder in their area. Confident and effective information exchange is the key to multi-agency working in any sphere - nowhere more so than in statutory partnerships for the reduction of crime and disorder. The effectiveness of information exchange arrangements is a reflection of the effectiveness of the partnership as a whole.

The purpose of this protocol is to facilitate and give guidance on how the exchange of personal and depersonalised information can be used to

- assist in reducing and preventing crime, disorder and substance misuse
- fulfil the *Prevent* duty outlined in the Counter Terrorism and Security 2015 Act
- support joint agency approaches to identifying and managing the risk of crime and disorder
- enable the parties to pool their expertise in assessing the nature and level of risk posed by potential offenders
- enable the parties to co-operate in averting identified risks of crime and disorder and its consequences
- reduce risk and fear experienced by staff, identified individuals and the public at large
- assist strategic planning
- help implement the provisions of the Crime and Disorder Act 1998 with particular regard to Section 17 and Section 115
- assist in the development of the Joint Oxfordshire Strategic Intelligence Assessment
- assist in the production of crime and disorder assessments for the purpose of preventing or detecting crime

1.2 Information Exchange

Information sharing involves a physical (electronic or paper) exchange of information between one or more individuals or agencies.

Data exchange seeks the same end, but relates more specifically to information recorded in a form that can be processed by equipment automatically, (usually electronically), in response to specific instructions.

If information is disclosed it must be stored securely and destroyed when no longer required for the purpose for which it was provided.

The 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 (For the purposes of this protocol, agency means agency signatory or organisation within the definition of the Data Protection Act 1998, and has been registered with the Information Commissioner for processing personal data). The identity of the originator must therefore be recorded against the relevant data. A recipient of such information must therefore obtain the consent of the original data owner before making a further disclosure.

Any disclosure of personal information must be bound to both common and statute law, for example, defamation, the common law duty of confidentiality, the Data Protection Act 1998 and the Human Rights Act 1998.

The protocol explains the principles that must be followed when exchanging information. This will apply to:

- any Order under the Crime and Disorder Act 1998
- the exchange of personal information following a conviction by a Court
- the exchange of information intended to support any action for the purposes of the Crime and Disorder Act 1998, namely the reduction or prevention of crime and disorder whether under this Act or other relevant legislation

The parties recognise that Section 115 of the Crime and Disorder Act 1998 can only be used to disclose information to an individual or group where that disclosure is necessary or expedient to support the local strategy to reduce crime and disorder, the youth justice plan, or any other purpose of the Act.

1.3 Benefits of information sharing

The benefits of sharing information are:

- Better informed decision making and joined up working.
- Improved inter-agency relationships.
- Better profiling of crime and disorder activity to enable the more effective targeting of resources.
- Reduction in crime and disorder.
- Regular monitoring and evaluation of community safety initiatives.

1.4 Principles of sharing information

Under the Data Protection Act 1998 personal information can usually be disclosed only to the person who is the subject of the information. However there are circumstances under which disclosure of personal information to other parties may be sanctioned.

Disclosure is considered to be a form of information processing under the Data Protection Act 1998. Under the Data Protection Act 1998 personal information needs to be processed fairly and lawfully, and should not be processed unless at least one condition from Schedule 2, and

for sensitive information one condition from Schedule 3 is met.

Consent is defined as “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”.
Many of the data protection issues surrounding disclosure can be avoided if the consent of the individual has been sought and obtained. However, if consent is being used as the basis for sharing information the individual must know precisely the data sharing that they are consenting to and the implications for them. They must also have genuine control over whether or not the data sharing takes place. Where there is no legal obligation or duty in place then consent should be sought in writing. Where oral consent is given a record of this should be made.

The following are alternative grounds to enable disclosure, which should be considered:

a. Public interest – disclosure can be considered if there is an over-riding public interest or justification for the disclosure. Whilst a disclosure in the public interest may be defensible in a particular case, this does not constitute a legal power to share data. It is desirable for any public body intending to disclose information on this basis to advise the data subject in time for them to make an application to the court, unless there are legal grounds for not doing so.

b. Non-disclosure exemptions under the Data Protection Act 1998 – exemptions under the Data Protection Act 1998 can be used to allow the disclosure of information. These can be used on a case by case basis and include exemptions for the prevention or detection of crime and in connection with any legal proceedings.

Extreme care and careful consideration should be taken where the disclosure of information includes details of witnesses, victims or from complainants and, wherever possible, consent from any identifiable third party should be sought.

Each agency must ensure that they are correctly registered with the Information Commissioner to share appropriate information under this protocol.

1.5 Conviction Data

Details of relevant convictions recorded on the Police National Computer, or retained on file by the parties to this protocol can be released to another Designated Officer to support proceedings under the Crime and Disorder Act 1998. However, it is recognised that care must be exercised in the disclosure of conviction data and a Designated Officer must ensure that the information is accurate and relevant to an enquiry before it is released.

2. The legal authority for sharing and exchanging information

2.1 The Data Protection Act 1998

This Act requires a structured approach to the handling of personal information and clear procedures need to be established by the Crime and Disorder Reduction Partnerships in Oxfordshire to ‘process’ this information.

Processing is defined by the Act and includes the 'obtaining', 'holding', 'using' and 'disclosing' of information. Depersonalised information is disclosed under the Crime and Disorder Act 1998, not the Data Protection Act 1998. Information can only be disclosed in appropriate circumstances and the information must be accurate, relevant, kept up to date, held no longer than necessary, and kept and exchanged securely.

Schedule 1 of the Data Protection Act 1998 includes eight principles in respect of the sharing of personal data:

1) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless;

    - at least one of the conditions in Schedule 2 is met; and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is met.

2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4) Personal data shall be accurate and, where necessary, kept up to date.

5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

6) Personal data shall be processed in accordance with the rights of data subjects under this Act.

7) 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 (i.e. data security).

8) 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.

2.2 Human Rights Act 1998

The Human Rights Act 1998 gives further effect in domestic law to articles of the European Convention on Human Rights. The Act requires all domestic law to be compatible with the convention articles. It also places a legal obligation on all public authorities to act in a manner compatible with the Convention. Should a public authority fail to do this then it may be subject of a legal action under section 7 of the Act. This obligation should not be seen solely in terms of an obligation not to violate convention rights but also as a positive obligation to uphold these rights.

This Act should be considered but does not necessarily present a major obstacle to legitimate information-sharing activity for the Crime and Disorder Reduction Partnerships in Oxfordshire. The Act needs to be taken into account in establishing whether the purpose of information exchange is lawful.

2.3 Common law duty of confidentiality

The duty of confidentiality has been defined by a series of legal judgments and is a common law concept rather than a statutory requirement. Personal data which is seen as subject to this duty includes information that is not already in the public domain, has a certain degree of sensitivity, or was provided on the expectation that it would only be used or disclosed for particular purposes. The Common Law judgments have identified a number of exceptions, which includes the need to prevent, detect and prosecute serious crime.

Where information is held in confidence e.g. as is the case with personal information provided to the National Health Service and medical practitioners by patients, the consent of the individual concerned should normally be sought prior to information being disclosed.

Where consent is withheld or is unobtainable, Designated Officers should assess on a case-by-case basis, whether disclosure is necessary to support action under the Crime and Disorder Act 1998 and whether the public interest arguments for disclosure are of sufficient weight to over-ride the duty of confidence.

The courts have ruled that the common law duty of confidence does not apply to information that has been effectively anonymised so that individuals cannot be identified. There is thus no barrier to the sharing of effectively anonymised data.

2.4 The Crime and Disorder Act 1998

Section 115 of the Crime and Disorder Act 1998 gave responsible authorities the power to share personalised information for the purposes of reducing crime and disorder.

Section 17 of the Crime and Disorder Act 1998 places a duty on each responsible authority to do all that it reasonably can to prevent, crime and disorder in its area.

The Police and Justice Act 2006 took forward many of the Crime & Disorder Act 1998 review recommendations including:

- Extending Section 17 of the Crime and Disorder Act 1998 to encompass anti-social behaviour, substance misuse and behaviour that adversely affects the environment.
- Introducing powers to make regulations providing a framework for minimum standards and information sharing.
- Repealing three yearly audits and strategies.
- Introducing a duty on responsible authorities to share depersonalised data, already held in a depersonalised format for the purposes of preventing crime and disorder in its area (Schedule 9(5) of the Police and Justice Act 2006).

These powers do not over ride other legal obligations such as compliance with the Data Protection Act 1998, the Human Rights Act 1998 or the common law of confidentiality.

2.5 Freedom of Information Act 2000

From 1st January 2005, any person under the provisions of this Act may request any information held by public sector authorities. Under certain circumstances an authority may refuse to supply information because they believe that one or more of twenty four possible exemptions may apply to the information being disclosed. For example, disclosure may breach other legislation such as the Data Protection Act 1998 or the

information may already be widely available in the public domain. Unless these exemptions apply, public authorities are obliged to provide the data within twenty working days of the receipt of a request.

Since the Data Protection Act 1998 will continue to govern access to personalised information, it is mainly non-personal data that will be affected by the provisions of the Freedom Of Information Act 2000. This will include data and information in any form, including informal, electronic and database records.

A request may be received by an authority for any information that it holds, not just that which it has generated itself or relates to its own activity. Should a request under the Freedom Of Information Act 2000 be received by one authority for information which originated with another authority, it is a requirement of this Information Sharing Protocol that the originating authority is consulted before any release is made. There may be specific reasons, such as public interest or the potential to compromise a third party, which may not be immediately evident.

The Freedom of Information Act 2000 is a complex piece of legislation. Almost all authorities have trained specific staff to deal with applications for information made under the Act. Their advice should be sought in the event of any questions arising about the Act.

The Police have their own particular rules on information sharing and retention as set out in the Code of Practice on the Management of Police Information (MoPI) and Authorised Processional Practice. It states that sharing police information must satisfy one of the following policing purposes;

- Protecting life and property
- Preserving order
- Preventing the commission of offences
- Bringing offenders to justice
- Duty under common or statute law (see section 2.3)
- Where there is any conflict between this protocol and the MoPI, the Police will regard MoPI as taking precedence

2.6 Other relevant Acts

Whilst the legislation highlighted in the sections above are the principal ones covering the exchange of information in respect of crime and disorder, there are a considerable number of other Acts that require or enable the sharing of information, including:

- Children Act 1989 and 2004
- Housing Act 1996
- Sexual Offences Act 2003
- Domestic Violence Crime and Victims Act 2004
- Offender Management Act 2007
- The Police and Justice Act 2006, and the Crime and Disorder (Overview and Scrutiny) Regulations 2009 made under the Act
- The Criminal Justice and Court Service Act 2000
- Policing and Crime Act 2009
- Police Reform and Social Responsibility Act 2011
- Legal Aid, Sentencing and Punishment of Offenders Act 2011

- Crime and Courts Act 2013
- Anti-Social Behaviour, Crime and Policing Act 2014
- Offender Rehabilitation Act 2014
- Counter Terrorism and Security Act 2015
- Serious Crime Act 2015
- Modern Slavery Act 2015

3. Security

3.1 General principles

BS7799 (British Standards Institution) and associated ISO (International Organisation for Standardisation) standards provides a baseline for security arrangements.

Agencies are working towards compliance with this standard. Partners should ensure they have appropriate security arrangements in place.

A key issue, especially for electronic documentation, is the consistent use of encryption – the National Health Service (NHS) has a mandate on encryption for identifiable data and secure information exchange. Unguarded exchange of personal information may not only infringe the rights of the individual subject or others that may be identifiable from the information, but also compromise the organisations sharing data or jeopardise any proceedings or legal measures based upon that information.

3.2 Secure information exchange

Transport and passing on of all personal information (held on paper or in electronic media), by any means including manual transport, fax or electronic mail, must be done in a secure manner.

Electronic Mail: E-mails containing confidential information must not to be sent to addressees outside of the organisation e-mail address book unless they have been sent via by an encrypted secure email facility (e.g. DX, PNN, PSN, GSX, GSI, CJSM, GCSX, CJSM, NHSnet, NHS [N3] Egress) with the appropriate protective marking. The use of password protected attachments to a non-secure/encrypted email facility is not permissible.

Faxing: should only be used in cases of operational emergency where other secure means of transfer are not available or timely. If used; specific faxing procedures must be followed.

- Check the recipient is present before you send the fax.
- Ensure the recipient is aware they should contact you if the fax has not been received.
- Use a fax cover sheet that contains the following confidentiality statement:

"This facsimile is to the above named addressee only. It may contain private and confidential information. If you are not the intended recipient you should not read, copy or use this fax in any other way. If you are unable to pass it onto the addressee please contact the sender and arrange to return it."

Telephone: Unless using a private secure network the telephone should only be used in cases of operational emergency.

Ensure that telephone conversations are conducted in an area where unauthorised persons cannot overhear them. Never discuss confidential information on mobile or cordless phones in a public area. When leaving a message, professionals (professionals refer to any officer who is handling data) should know who they are leaving a message with before passing confidential information.

Postal Mail: Outgoing confidential information should be marked 'Confidential and Private'. Information to be sanitised where possible and sent in non-GPMS marked sealed envelope with the senders address on the back. For police data use TVP approved secure couriers.

Oxfordshire County Council Approved couriers are as follows;

- Swift 24 hour Courier Service
- QED Sameday Courier
- City Sprint
- Parcel Force

Thames Valley Police Approved courier is City Link.

Hand Delivery: In a sealed envelope to a specified and trusted person from the receiving partner agency

3.3 Security classifications

Security classifications indicate the sensitivity of information in terms of likely impact resulting from compromise, loss or misuse.

All information exchanged should be classified using either the Government Protective Marking Scheme (which Thames Valley Police and Oxfordshire County Council use) or the recently launched replacement Government Security Classification scheme (all other statutory partners). Both of these schemes set out information handling requirements to ensure that proportionate and effective security controls are in place, according to the sensitivity of the information. See Appendix B for further information.

There are also varying security measures which must be in place to protect types of information. For example 'Restricted' information when not in use must be stored in a locked container within a secure environment.

If you are uncertain which classification to use or the method of seek advice of the Thames Valley Police Information Security Officer on 01865 846594 or contact the Oxfordshire County Council ICT Service desk on 0845 052 1000 to log an enquiry with the ICT Business Delivery Team.

3.4 Secure information storage and retention

Paperwork must be dated, marked as confidential and organised.

Electronic files should be dated, encrypted if stored on any drive with general access, and viewed through a PC with password protection.

Verbally exchanged information should be secure from eaves-dropping and recorded/validated as soon as possible. Verbal information should be subject to the same considerations as written, and should not be exchanged unless both parties are satisfied that the request is legitimate and there is a good reason for not pursuing a written route.

All records should be managed and reviewed to ensure that currency is

maintained and that nothing is retained longer than required for the specific purpose that led to its exchange. Paper records should be shredded and electronic records should be double deleted. All agencies should have internal procedures regarding data protection and requests which should also be observed.

4. Data Standards

There is a requirement that information must be accurate and complete before it can be made available to other members of the partnership. BS7666 is the standard for describing locations such as addresses, rights of way and streets. Most information in the public sector has a location element to it so it is appropriate to use the BS7666 standard in order to convert disparate data sets from different systems and agencies and fully integrate them.

5. Indemnity

5.1 Receiver and Supplier

In consideration of the provision of information in accordance with this protocol any party to this protocol who receives information under this protocol "the Receiver" from any other party "the Supplier" undertakes to indemnify the Supplier against any liability which may be incurred by the Supplier arising from or in any way connected with the acts or omissions listed un paragraph 5.3 bellow on the part of the Receiver.

5.2 Indemnity statement

The parties to this protocol undertake to fully indemnify and keep indemnified all other agencies and/or persons to this protocol from and against any and all loss, damage or liability (whether criminal or civil) suffered and legal fees and costs incurred by other agencies resulting from any negligent act or omission and/or breach of this protocol by the indemnifying agency including:

- Any act or omissions outlined in paragraph 5.3 negligent or default of indemnifying agencies, employees or agents; or
- Breaches resulting in any successful claim by any third party arising out of the wrongful disclosure of any information by the indemnifying agency.

5.3 Acts or Omissions

The acts or omissions referred to in paragraphs 5.1 and 5.3 are;

- Information for purposes other than those specified in the Oxfordshire Information Sharing Protocol or associated information sharing schedule, or for purposes other than disclosed on the record of request or disclosure.
- Disclosure of the information to a third party except as is specified in the Oxfordshire Information Sharing Protocol.
- Wilful misconduct or negligence in the handling, keeping or disposal of the information.
- A supplier must indemnify the receiver to the extent that the information received has been released in accordance with the law.
- Loss or compromise of information whilst in the receiver's custody or control.
-

6. Media Strategy

The parties to this protocol will subscribe to the following principles when discussing with the media issues which have arisen from the initial review of crime and disorder, the summary produced for the purpose of public consultation or the final crime reduction strategy: -

We agree when handling the media,

- To be fair to our fellow partners, and maintain their integrity.
- When providing information to the public, to do so honestly and fairly.
- Statements must reflect the multi-agency decision process.
- Consent of the data controller will be sought prior to release to the media where practicable, individual data subjects will be consulted if the media coverage was such that it may identify the individual (circumstances may exist that make this impractical, such as where the current whereabouts of the data subject is unknown, or the purpose of the media coverage is to identify the individual data subject).
- All organisations should be aware of requirements in terms of media strategy and protocol.

Press and public relations staff in each organisation should have working knowledge of the structure, key issues and staff in other partner organisations. Opportunities for the placement of stories in organisational publications should be encouraged.

Section 2

The Information Exchange Process

7. Agencies involved in information sharing

Community Safety Partnerships (previously called Crime and Disorder Reduction Partnerships (CDRPs) are defined in the Crime and Disorder Act 1998 as:

> *"An alliance of organisations which generate strategies and policies, implement actions and interventions concerning crime and disorder within their partnership area".*

7.1 Responsible Authorities

Under Section 5(1) of the Crime and Disorder Act 1998 the following organisations are named as responsible authorities:

- District or borough council, unitary authority or county council.
- Police Force
- Fire Authority (as amended under the Police Reform Act 2002)
- Clinical Commissioning Group (as amended under the Health and Social Care Act 2012).
- Community Rehabilitation Company (as amended Policing and Crime Act 2009 and updated according to the Transforming Rehabilitation Strategy)
- The National Probation Services (amended under the Policing and Crime Act 2009 and updated according to the Transforming Rehabilitation Strategy)

7.2 Co-operating Bodies

Section 5(2)(c) of the Crime and Disorder Act 1998 provides details of persons or bodies required to co-operate with the responsible authorities in their exercise of the functions conferred by Section 6 of that Act. The following persons or bodies have been prescribed by order of the Secretary of State;

- Parish Councils
- NHS Foundation Trusts
- Governing bodies of schools
- Proprietors of independent schools
- Governing bodies of an institution within the further education sector
- Social landlords
- Police and Crime Commissioner (Police Reform and Social Responsibility Act)

7.3 Invitees to participate

Section 5(3) of the Crime and Disorder Act 1998 provides descriptions of persons or bodies, at least one of which must be invited by the responsible authorities to participate in the exercise of the functions conferred by Section 6 of that Act (primarily the development and delivery of a partnership strategy for the reduction of crime and disorder and tackling drug abuse). A full list can be found in Appendix C.

7.4 Duty to share depersonalised information

Section 17 of the Crime and Disorder Act 1998 places a duty on each responsible authority to do all that it reasonably can to prevent, crime and disorder in its area. In addition to this, Schedule 9(5) of the

Police and Justice Act 2006 strengthens this by introducing a duty on the same agencies to share depersonalised information these purposes.

The minimum requirements for sharing depersonalised data are set out in the Crime and Disorder (prescribed information) Regulations 2007 (Statutory Instrument 1831) - see Appendix A.

7.5 Powers to share personal information

Under Section 115 of the Crime and Disorder Act 1998, partners have the power to share personal information already held if it is necessary to support the local Community Safety Strategy, reduce crime or other conditions in the Act. It does not impose a requirement on them to exchange personal information and responsibility for disclosure remains with the agency that holds the data.

In the absence of a statutory gateway to disclose, the disclosing agency must be confident that, on balance (assuming there are no statutory restrictions on disclosure), there is an overriding public interest in the disclosure.

Persons or bodies signed up to the protocol will therefore not automatically have the power to send or receive all information. By signing up to the protocol they are agreeing to the overarching information sharing principles and not that that information must be shared with them. Specific information sharing schedules annexed to the Protocol will detail the specific purposes and the processes involved in the sharing of personal and de-personalised types of information exchanged.

For the purposes of this protocol and in support of the strong community safety partnership working in Oxfordshire the signatories to this protocol will be as extensive as necessary to reduce crime, disorder and administer justice in Oxfordshire.

Each organisation must provide a main signatory at Chief Executive or such appropriate level. By signing up to the Protocol they also agree to the indemnity provision in section 5.2.

7.6 Responsibilities of signatories

It is the responsibility of these signatories to ensure that:

- they have read and understood the guiding principles outlined in Information Sharing Protocol;
- the data protection principles are upheld and the information shared is kept secure and confidential;
- a mechanism exists by which the flow of information can be controlled;
- adequate arrangements exist to test adherence to the protocol;
- any electronic information exchange is fully secure;
- identify Designated Officer(s) from within their organisation who will process/initiate information requests;
- appropriate training for Designated Officers is provided on the guiding principles outlined in the ISP;
- Agree associated information sharing schedules relevant to their organisation

Organisational signatories will be sort and maintained by the relevant Community Safety Partnership (CSP). Agreement

must be sort via the CSP to enable for organisations to sign up to the protocol.

7.7 Involvement of external agencies in the protocol

This protocol does not cover every exchange of information. Release of information for analysis and evaluation by researchers, (by universities or consultants), or subcontractors requires a formal written agreement. Responsibility for ensuring compliance rests with the agency that subcontracts the work. They must ensure that the subcontractor is obliged to fully comply with the relevant legislation. Agencies should also ensure that they have effective data security systems in place for responding effectively and safely to other requests for personal information that may be made by bodies such as the Police, Social Services or Housing, in pursuit of their main business. Although the principles on which this Information Sharing Protocol is based will still apply, appropriate internal procedures should also be in place.

7.8 Information exchange outside Oxfordshire

There will be occasions when agencies within Oxfordshire may need to make (or may receive) requests for personal information from agencies operating outside the county. With due regard to the Data Protection Act 1998 restriction confining information exchange to the European Economic Area (the NHS has further restricted this to the UK recently), the principles of this protocol continue to apply and exchange should take place between appropriate Designated Officers in the areas.

7.9 Confidentiality Statement

The information exchanged under this protocol will only be used for the purpose for which it was requested, and it will be securely exchanged, stored and destroyed when no longer required. All agencies that are part of the information sharing process will, upon signing this protocol, are bound to comply with its terms.

8. Designated Officers (DO)

The signatory agencies will nominate Designated Officers (DO), part of whose function is to process or initiate requests for any information. The DO may also initiate information sharing schedules which will then be annexed to this protocol (see Appendix E).

The DO must have an understanding of the legislation governing data exchange as described in this Protocol and by the Information Commissioner's Office. They must also have signed a Confidentiality Agreement (as shown in Appendix F).

Where a DO has initiated an associated information sharing schedule they are also responsible for maintaining a full list of the entire nominated DO identified within the schedule. They must ensure that the full list is maintained and circulated to those identified DO. They must ensure that all DO sign the confidentiality agreement and retain a copy of these (see Appendix F).

Any new or amended information sharing schedule must be agreed by the relevant Community Safety Partnership.

No officer shall be permitted to request or disclose information in respect of another department for which he or she is not the DO unless he or she has the written consent of the particular DO concerned.

Any authorisation given by a party to a DO listed shall automatically end upon the DO ceasing to be employed by the party who appointed him.

The DO who initiated an information sharing schedule must notify all associated DO of any change; either to the schedule or of identified DO.

The parties authorise the DO to request and disclose information to the bodies or parties identified in this protocol in accordance with the provisions of the Crime and Disorder Act 1998 and the Data Protection Act 1998 during the time that they are in the employment of the nominating party or are acting on its behalf.

9. Information disclosure and exchange

Any person requesting information from another agency under this protocol must submit the request through a DO. No information shall be disclosed to any other person other than the nominated DO or those parties identified in an information sharing schedule.

All requests should be acknowledged and returned within 10 working days. Where any request cannot be dealt within these time limits the DO shall notify the requesting party immediately the delay is known. When making the application the requesting party shall notify the data owner of any time restrictions on the supply of data e.g. Court dates.

The considerations and security around disclosure and exchange of information apply equally to paper and electronic records. All considerations and procedures around the secure exchange and principles of evaluation of requests and retention of information in this Information Sharing Protocol apply to all exchanges, irrespective of medium.

It is the responsibility of the DO to record the exchange of information. Records should be kept in such a way that they could be subject to audit.

The DO must; either jointly or alone, determine the purpose for which the information is to be processed applies according to the protocol or associated information sharing schedule.

9.1 Information process and information sharing schedules

All information exchanges must have an associated *information sharing* schedule (see Appendix E). The schedule must meet the requirements as set out in this protocol.

Regular data or information exchanges for the purpose of crime and disorder analysis may relate to one information sharing schedule that specifies how the information will be regularly processed

A DO may initiate a schedule but it must be also be agreed by the relevant Community Safety Partnership and signed off by the Organisational Signatories that apply to that particular schedule.

The DO or Organisational Signatory initiating the schedule must hold the original document including all signed Confidentially Agreements.

Each Community Safety Partnerships (CSP) must agree and hold a log of all

information sharing schedules under this protocol that are relevant to their area. Any information schedule that has not been agreed by the relevant CSP will be invalid. Information sharing schedules must be reviewed every three years.

An information sharing schedule should be completed for the exchanges of information. All officers accessing the information must be identified within the schedule and also have signed the Confidentiality Agreement.

10. Complaints and Breaches

10.1 Complaints

The relevant Community Safety Partnership will record all complaints relating to the schedules that they manage, regardless of how they are received. They will ensure that all of the relevant partners are notified in writing and the partner organisation's complaints procedure will be applied.

Every effort will be made within the guidelines of the Data Protection Act 1998 to assist with the investigation of any complaint. Individuals do retain the right to raise a complaint with such bodies as the Information Commissioner or the statutory Ombudsman.

10.2 Breaches

We agree that any breach of confidentiality will seriously undermine and affect the credibility of crime audit work, our partnership objectives and render us liable for breach of the law. All DO and other professionals identified under each schedule are required to sign a Confidentiality Agreement that describes the sanctions that maybe applied if a breach is committed.

We undertake at all times to comply with data protection and other legal requirements relating to confidentiality.

11. Subject and Third Party Data

Under the terms of the Data Protection Act 1998, any individual has the right to request access to information held about them and this would include information held for community safety purposes. An individual may make a subject access request under the provisions of the Data Protection Act 1998 using the existing mechanisms and forms of each agency.

If an agency receives a subject access application, they need to consider whether the information can be provided, or whether an exemption under the Data Protection Act 1998 needs to be applied to enable the request to be denied. Examples where an exemption might apply would include where the data cannot be supplied without identifying a third party, or where disclosure would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

Where a third party can be identified from the information, the agency is not obliged to comply with the request unless:

- The other individual has consented in writing to the disclosure of the information to the person making the request, or;
- It is reasonable in all the circumstances to comply with the request without the consent of the other individual.

- The third party information can be redacted to prevent the identification of the third party to enable disclosure.

If the personal data requested is identified as belonging to another agency, it will be the responsibility of the receiving agency to either forward on the request to the data owner or contact them to determine whether the latter wishes to claim an exemption under the provisions of the Data Protection Act 1998.

If, in the judgement of the Data Controller there are grounds for an exemption under the provisions of the Data Protection Act 1998, a mandate endorsing this decision should be obtained from the agency's Data Protection Officer.

All agencies need to co-operate speedily to ensure that requests are met within the statutory time period set out in the Data Protection Act 1998.

12. Review

This protocol and all annexed information sharing schedules will be reviewed every three years or sooner if relevant developments or issues dictate. It will be the responsibility of the Oxfordshire safer Communities Partnership who responsible for the protocol to initiate the review.

A copy of all amended information sharing schedules and associated confidentiality agreements must be agreed by the relevant Community Safety Partnership to validate them for inclusion in the protocol.

.

Section 3

Appendices

Appendix A

Crime and Disorder (Prescribed Information) Regulations 2007

List of Depersonalised Information

1. Information held by the police force for the area on the category of each:
   - Anti–social behaviour incident
   - Transport incident
   - 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 2007-2008, and the time, date and location of each of those incidents.

2. Information held by the police force for the area on the sub-category of each crime classified as:
   - Burglary
   - Criminal damage
   - Drug offences
   - Fraud and forgery
   - Robbery
   - Sexual offences
   - Theft and handling stolen goods
   - Violence against the person
   - Other offences

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

3. Information held by the fire and rescue authority for the area on the time, date and location of each:
   - deliberate primary fire (excluding deliberate primary fires in vehicles) in the area,
   - deliberate primary fire in vehicles in the area,
   - deliberate secondary fire (excluding deliberate secondary fires in vehicles),
   - incident of violence against employees of the fire and rescue authority in the area, and
   - fire in a dwelling in the area where no smoke alarm was fitted attended by fire and rescue services of the authority, as defined in accordance with Fire Statistics, United Kingdom 2005

4. Information held by the fire and rescue authority for the area on the time and date of each call to the fire and rescue services in the area in relation to a malicious false alarm and the purported location of those alarms as defined in accordance with Fire Statistics, United Kingdom 2005.

5. Information held by the local authority for the area on the time, date and location of each road traffic collision in the area and the number of adults and children killed, seriously injured and slightly injured in each of those collisions.

6. Information held by the local authority for the area on the age and gender of each of the pupils subject to a permanent or fixed term exclusion from state primary and secondary schools in the area, the names and addresses of the schools from which those pupils have been excluded and the reasons for their exclusion.

7. Information held by the local authority for the area on the time, date and location of racial incidents.

8. Information held by the local authority for the area on the category, time, date and location of each:
   - incident of anti-social behaviour identified by the authority, and
   - incident of anti-social behaviour reported to the authority by the public, 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 2007-2008 or any other system for classifying anti-social behaviour used by that authority as at the date of these Regulations.

9. Information held by each Clinical Commissioning Group the whole or any part of whose area lies within the area on the general postcode address of persons resident in the area admitted to hospital, the date of such admissions and the sub-categories of each admission within the blocks:
   - assault (X85-Y09),
   - mental and behavioural disorders due to psychoactive substance use (F10-F19)
   - toxic effect of alcohol (T51),and
   - 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) classified in accordance with the International Classification of Diseases, Tenth Revision (ICD-10) published by the World Health Organisation.

10. Information held by each Clinical Commissioning Group the whole or any part of whose area lies within the area on the general postcode address of persons resident in the area admitted to hospital in respect of domestic abuse as defined in Section 2.2 of the Responding to domestic abuse: a handbook for health professionals published by the Department of Health in December 2005, and the date of such admissions.

11. Information held by each Clinical Commissioning Group the whole or any part of whose area lies within the area on the number of :
    - mental illness outpatient first attendances and,
    - persons receiving drug treatment, in the area.

12. Information held by each Clinical Commissioning Group the whole or any part of whose area lies within the area on the location, time and date of ambulance service calls to incidents relating to crime and disorder and the category of such incidents using any system for classifying crime and disorder used by that authority.

Appendix B

Government Protective Marking (GPMS and GSC)

The UK Government has introduced a simplified and less bureaucratic three-tier Security Classification Scheme from 02 April 2014 which has been adopted by most statutory partners. Police Forces will phase the implementation, subject to confirmation of adoption, from mid-2015 onwards. It is likely that when sharing information within the Community Safety Partnership partners will be working with both schemes in parallel for an interim period. The below information may serve as helpful guidance during this period.

Government Protective Marking Scheme

The criteria for the Government Protective Marking Scheme are as follows;

Criteria for assessing PROTECT:

- Cause distress to individuals.
- Breach proper undertakings to maintain the confidence of information provided by third parties.
- Breach statutory restrictions on the disclosure of information.
- Cause financial loss or loss of earning potential, or to facilitate improper gain.
- Unfair advantage for individuals or companies
- Prejudice the investigation or facilitate the commission of crime.
- Disadvantage the government in commercial or policy negotiations with others.

Criteria for assessing RESTRICTED:

- Affect diplomatic relations adversely.
- Cause substantial distress to individuals.
- Make it more difficult to maintain the operational effectiveness or security of United Kingdom or allied forces.
- Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies.
- Prejudice the investigation or facilitate the commission of crime.
- To breach proper undertakings to maintain the confidence of information provided by third parties.
- Impede the effective development or operation of government policies.
- To breach statutory restrictions on disclosure of information
- Disadvantage government in commercial or policy negotiations with others
- Undermine the proper management of the public sector and its operations.

Criteria for assessing CONFIDENTIAL:

- Materially damage diplomatic relations (i.e. cause formal protest or other sanction).

- Prejudice individual security or liberty.
- Cause damage to the operational effectiveness or security of United Kingdom or allied forces or the effectiveness of valuable security or intelligence operations.
- Work substantially against national finances or economic and commercial interests.
- Substantially undermine the financial viability of major organisations
- Impede the investigation or facilitate the commission of serious crime.
- Impede seriously the development or operation of major government policies.
- Shut down or otherwise substantially disrupt significant national operations.

Criteria for assessing SECRET:

- Raise international tension.
- Damage seriously relations with friendly governments
- Threaten life directly, or seriously prejudice public order, or individual security or liberty.
- Cause serious damage to the operational effectiveness or security of United Kingdom or allied forces or the continuing effectiveness of highly valuable security or intelligence operations.
- Cause substantial material damage to national finances or economic and commercial interests.

Criteria for assessing TOP SECRET:

- Threaten directly the internal stability of the United Kingdom or friendly countries.
- Lead directly to widespread loss of life.
- Cause exceptionally grave damage to the effectiveness or security of United Kingdom or allied forces or to the continuing effectiveness of extremely valuable security or intelligence operations.
- Cause exceptionally grave damage to relations with friendly governments.
- Cause severe long-term damage to the United Kingdom economy.

The new Government Security Classification scheme (Launched in April 2014)

Under the new scheme the classification levels are as follows:

- there is no unclassified level.
- **OFFICIAL** - *any* information that is created, processed, generated, stored or shared within (or on behalf of) Government.
- **SECRET** – very sensitive information that justifies heightened protective measures to defend against determined and highly capable threats. Examples include investigation reports of serious or organised crime or intelligence operations.
- **TOP SECRET** - the most sensitive information requiring the highest levels of protection from the most serious threats. This includes information where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations.

Working with existing and new classifications:

The majority of existing information will be treated as OFFICIAL, and should be supplied with any specific handling instructions that are required. Information marked as OFFICIAL that requires more prescriptive handling requirements or a reduced audience due to its sensitivity, may be marked with a caveat of 'OFFICIAL – Sensitive'. As with the old scheme, a very small proportion of the information received will remain either SECRET or TOP SECRET. Although there is no direct mapping between the old and new the table below illustrates the most likely relationship between the old and new classifications.

Existing Classification (GPMS)	Not Protectively Marked	PROTECT	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
New Classification (GSC)	OFFICIAL				SECRET	TOP SECRET

Appendix C

Invitees to participate (Section 5(3) of the Crime and Disorder Act 1998)

Section 5(3) of the Crime and Disorder Act 1998 provides descriptions of persons or bodies, at least one of which must be invited by the responsible authorities to participate in the exercise of the functions conferred by Section 6 of that Act (primarily the development and delivery of a partnership strategy for the reduction of crime and disorder and tackling drug abuse). The following persons or bodies have been prescribed by order of the Secretary of State.

- Drug and Alcohol Teams
- Training and Enterprise Councils
- Voluntary Organisations – whose objects are to provide assistance to young persons via youth work/ informal education.
- Crown Prosecution Service
- Crown Court Manager
- Magistrates Court Committee
- Representative of Neighbourhood Watch Schemes
- Victim Support Scheme member
- Service Police
- Ministry of Defence Police
- Bodies providing School transport.
- Bodies providing and operating public transport
- Passenger Transport Executives and Authorities
- Bodies providing services to women, young, elderly, physically and mentally disabled, those of different racial groups, homosexuals and residents
- Bodies established for religious purposes
- A company or partnership which has a place of business within that area
- Bodies established to promote retail business
- Trade union
- Registered Medical practitioner providing general or personal medical services in that local government area
- Bodies representing medical practitioners
- Higher education governing body
- British Transport Police
- Environment Agency

Appendix D

Glossary

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

Incident

Is defined as any act that is a suspected crime, suspicious activity, unusual or disorderly activity

Anti-social behaviour

The definition stated in the Crime and Disorder Act 1998 is “behaviour which causes or is likely to cause harassment, alarm, or distress to one or more people who are not in the same household as the perpetrator”

Terrorism

The Terrorism Act 2000 defines terrorism as an action that endangers or causes serious violence to a person or people; causes serious damage to property; or seriously interferes or disrupts an electronic system. The threat must be designed to influence the government or to intimidate the public to advance a political, religious or ideological cause.

Radicalisation

The Prevent duty guidance (2015) defines radicalisation as the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups.

Designated Officer (DO)

The person or persons who either jointly or alone determines the purposes for which personal information is processed

Disorder

Refers to the level or pattern of anti-social behaviour within a particular area

Depersonalised (Non personal or Anonymised) information

Depersonalised information is defined as information where any reference to or means of identifying a living individual has been removed. This is any information, which does not (or cannot be used to) establish the identity of a living individual. There are no legal restrictions on the exchange of depersonalised information

Data in the public domain

This type of information incorporates any information, which is publicly available, whether it relates to an individual or not.

ISOBased in Geneva, the ISO, or to give it it's longer name "International Organization for Standardisation" is an international standard setting organisation and the world's largest publisher of industrial and commercial standards. The ISO consists of a network of National Standards Institutions from 162 member countries, including Britain and The British Standards Institute (BSI).

Personal information

Personal information means information, which relates to a living individual who can be identified either:

- Directly from the information or
- From the information and any other information which is in the possession of or is likely to come into the possession of the data controller
- and which affects their privacy, whether in personal or family life, business or professional capacity

Sensitive personal information

Is defined as information describing:

- Mental and physical health
- Racial or ethnic origin
- Religious beliefs or beliefs of a similar nature
- Sexual life
- The commission or alleged commission of any offence
- Political opinions
- Membership of a Trade Union

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

Appendix E

Information Sharing Schedule

The information exchange process is subject to the provisions of the Data Protection Act 1998 and the common law duty of Confidentiality. The information must not be used for any purpose other than that for which it is requested and must not be disclosed to an unauthorised person.

The powers to exchange information and the process for exchanging information for the purpose of community safety are described in the associated Oxfordshire Safer Communities Partnership Information Sharing Protocol.

No information is to be accessed or shown to individuals who have not agreed and signed the Confidentiality Agreement. Any breach in confidentiality may result in sanctions described with the Confidentiality Agreement (see Appendix F of the Protocol). No information provided by partners to those procedures will be released to any third party without the permission of the owning partner.

A copy of this Information Sharing Schedule and any amendments must be agreed by a Community Safety Partnership (CSP) and all relevant parties Should this Schedule be terminated the instigating Designated Officer must notify the CSP and all relevant parties.

Post of Designated Officer instigating this procedure			
Post of Designated Officer			
Date instigated		**Review date**	
Schedule title			
Purpose of this information sharing process			
(Please show how personal information is necessary or expedient for crime reduction purposes. Without this information, the process may be held up)			
Types of information exchanged under this Information Sharing Procedure			

Transmission, storage and retention period of data exchanged under this information sharing process		
Other officers identified for this information sharing process		
I have read and understand the ISP and Confidentiality Agreement		
Name	**Post**	**signed**

For Office use only

Organisational Signatories agreed ☐ Schedule meets ISP Requirements ☐

Copy all Confidentiality Agreements received ☐

Schedule Reference	
Organisation holder	
Initiating Designated Officer	
Review date	

Appendix F

Confidentiality Agreement for Designated Officers

Signatories of the Official Secrets Act 1911-89

I understand that as a signatory of the Official Secrets Act 1911-89 (the Acts) I will be subject to the restrictions and duties imposed by the Acts and that disclosure of any information, document, or article (or part thereof) in breach of the provisions of the Acts will make me liable to prosecution.

Non-signatories of the Official Secrets Act 1911-89

I have been informed that information, documents or other articles protected against disclosure by the provisions of the Official Secrets Act (for example relating to the prevention and detection of crime) will come into my possession in circumstances requiring it to be held in confidence. I understand that I may be prosecuted for an offence under the Official Secrets Acts 1911-89 should I disclose without lawful authority any such information, documents or other articles.

I understand that on termination of my employment, contract or other work with the organisations in whose employment I was in when I signed the Acts, the restrictions on disclosure of information under the Acts, and liability to prosecution, continue to apply.

Data Protection Act 1998

I understand that the Data Protection Act 1998 establishes principles that govern the manner in which personal data is used, including requirements that data is:

- Obtained and processed fairly and lawfully
- Held only for a specified and lawful purpose
- Not used or disclosed other than as authorised.

I also understand that I am liable to prosecution if I knowingly or recklessly use, obtain, disclose or transfer data without authority or other lawful reason.

Confidentiality Declaration

I understand that information coming into my possession or knowledge is as a consequence of the Oxfordshire Safer Communities Partnership Information Sharing Protocol and/or associated information sharing schedule. The information I receive will be held in confidence and must only be used as authorised in connection with the purposes of this process, for the prevention or detection of crime, or the administration of justice. I understand that the unauthorised communication of any such information to any person, either verbally or in writing, could result in dismissal, termination of contract, civil liability, and/or prosecution.

Associated Schedule Title**:** _____

Name _____ Signature _____ Date _____

Job title _____ Organisation _____

Appendix G

Oxfordshire Safer Communities Partnership (OSCP) Information Sharing Protocol (ISP) Agreement for Additional Organisation Signatories

Signatory Organisations Responsibilities

Each organisation must provide a main signatory at Chief Executive or such appropriate level. By signing up to the Protocol they agree to the indemnity provision (Section 5 of the ISP).

It is the responsibility of these signatories to ensure that:

- they have read and understood the guiding principles outlined in Information Sharing Protocol;
- they have signed the Confidentiality Agreement;
- the data protection principles are upheld and the information shared is kept secure and confidential;
- a mechanism exists by which the flow of information can be controlled;
- adequate arrangements exist to test adherence to the protocol;
- any electronic information exchange is fully secure;
- identify Designated Officer(s) from within their organisation who will process/initiate information requests;
- appropriate training for Designated Officers is provided on the guiding principles outlined in the ISP.

Confidentially Agreement

Signatories of the Official Secrets Act 1911-89

I understand that as a signatory of the Official Secrets Act 1911-89 (the Acts) I will be subject to the restrictions and duties imposed by the Acts and that disclosure of any information, document, or article (or part thereof) in breach of the provisions of the Acts will make me liable to prosecution.

Non-signatories of the Official Secrets Act 1911-89

I have been informed that information, documents or other articles protected against disclosure by the provisions of the Official Secrets Act (for example relating to the prevention and detection of crime) will come into my possession in circumstances requiring it to be held in confidence. I understand that I may be prosecuted for an offence under the Official Secrets Acts 1911-89 should I disclose without lawful authority any such information, documents or other articles.

I understand that on termination of my employment, contract or other work with the organisations in whose employment I was in when I signed the Acts, the restrictions on disclosure of information under the Acts, and liability to prosecution, continue to apply.

Data Protection Act 1998

I understand that the Data Protection Act 1998 establishes principles that govern the manner in which personal data is used, including requirements that data is:

- Obtained and processed fairly and lawfully
- Held only for a specified and lawful purpose
- Not used or disclosed other than as authorised.

I also understand that I am liable to prosecution if I knowingly or recklessly use, obtain, disclose or transfer data without authority or other lawful reason.

Confidentiality Declaration

I understand that information coming into my possession or knowledge is as a consequence of the Oxfordshire Safer Communities Partnership Information Sharing Protocol and/or associated Schedule. The information I receive will be held in confidence and must only be used as authorised in connection with the purposes of this process, for the prevention or detection of crime, or the administration of justice. I understand that the unauthorised communication of any such information to any person, either verbally or in writing, could result in dismissal, termination of contract, civil liability, and/or prosecution.

Information Sharing Protocol Agreement Declaration

I have read the Oxfordshire Safer Communities Partnership Information Sharing Protocol and understand the responsibilities and confidentiality agreement outline above.

Name		Signature		Date	
Job title		Organisation			

Appendix H

Roles & duties according to the OSCP ISP

Signatory Organisations

Each organisation must provide a main signatory at Chief Executive or such appropriate level. By signing up to the Protocol they agree to the indemnity provision (part 5 of the ISP).

It is the responsibility of these signatories to ensure that:

- they have read and understood the guiding principles outlined in Information Sharing Protocol;
- the data protection principles are upheld and the information shared is kept secure and confidential;
- a mechanism exists by which the flow of information can be controlled;
- adequate arrangements exist to test adherence to the protocol;
- any electronic information exchange is fully secure;
- identify Designated Officer(s) from within their organisation who will process/initiate information requests;
- appropriate training for Designated Officers is provided on the guiding principles outlined in the ISP;
- Agree associated information sharing schedules relevant to their organisation

Organisational signatories will be sort and maintained by the relevant Community Safety Partnerships or the Oxfordshire Safer Communities Partnership.

Designated Officer(s)

Any authorisation given by a party to a Designated Officer shall automatically end when the Designated Officer ceases to be employed by the party that appointed them.

It is the responsibility of the Designated Officer to ensure that:

- they have read and understand guiding principles outlined in the Information Sharing Protocol;
- they have signed the Confidentiality Agreement (see appendix F);
- ensure exchanges of information are recorded using an associated Information Sharing Schedule (blank form in appendix E);
- determine the purpose for which the information is to be processed and applies according to the Information Sharing Protocol and Information Sharing Schedule;
- not to disclose information/data to any other person other than the nominated Designated Officer identified within the associated Information Sharing Schedule;

- acknowledge and returned all requests within 10 working days. Where any request cannot be dealt within these time limits they shall notify the requesting party immediately of the delay; and
- record the exchange of information in such a way that they could be subject to audit;

DMO responsible for initiating schedule

- ensure that new or amended information sharing schedules have been agreed by a Community Safety Partnership
- ensure that information sharing schedules annexed to the protocol are reviewed every three years.
- ensure that all signatories related to the schedule are aware of its purpose
- ensure that all signatories related to the schedule have read and understood the confidentiality agreement
- maintain a record of the information sharing schedule and of designated officers related to the schedule.
- Ensure that changes to the information sharing schedule including designated officers associated with the schedule are circulated immediately to the all the listed designated officers.

Community Safety Partnerships (CSP)

Each CSP is responsible for the information sharing schedules under the protocol that are relevant to their area. It is the responsibility of the CSP to ensure that:

- Information sharing schedules are appropriate and have all the relevant signatories and confidentially agreements;
- hold a record of all the information sharing schedules under this protocol that are relevant to their area.
- ensure information sharing schedules are reviewed every three years or otherwise required.
- ensure organisational signatories agree and sign up to the ISP and the relevant schedules.
- maintain a list of organisational signatories and copies of their signed agreements.
- record all complaints relating to the schedules that they manage and ensure that all of the relevant partners are notified in writing of the complaint.
-

The Oxfordshire Safer Communities Partnership (OSCP)

The Oxfordshire Safer Communities Partnership is responsible for overall the management of the Information Sharing Protocol. It is the responsibility of the OSCP to ensure that the ISP is reviewed every three years or sooner if relevant developments or issues dictate.