

IS



**GENERIC INFORMATION SHARING
PROTOCOL**

Between

Lincolnshire Police

and

<<Partner Agency/Organisation>>

TABLE OF CONTENTS

Table of Contents 2

Purpose of this Protocol 3

 Introduction..... 3

 Purpose..... 3

Exchanging Information and Disclosure 3

 Information Exchange 3

 Disclosures 4

 Consent..... 4

 Reasons for Information Exchange 4

 Benefits of information exchange 4

 Witnesses, Victims and Complainants 5

Responsibilities of Signatories..... 5

Designated Officers/ Management Co-ordination..... 6

Information Security..... 6

 Security – General..... 6

 IT Security Requirements for Police Provided Information. 6

 Physical Security Requirements for Police Provided Information 7

 Personnel Security 8

 Information Breaches..... 8

 Subject Access 9

 Confidentiality Agreement 9

Vetting 9

Disclaimer..... 10

Indemnity 10

Reviews 10

Signatures 11

PURPOSE OF THIS PROTOCOL

Introduction

The purpose of this protocol is to facilitate the lawful exchange of data in order to comply with the statutory duty on Chief Police Officers and relevant agencies to work together for the purpose of implementing strategies and tactics in relation to crime reduction and the prevention and detection of crime throughout Lincolnshire.

Purpose

The Crime and Disorder Act 1998 and the Police Reform Act 2002 places obligations on various agencies as defined in the legislation to co-operate in the development and implementation of a strategy for addressing the issues relating to crime and disorder in their area.

Effective information exchange is the key to partnership working. The effectiveness of information exchange is a reflection of the effectiveness of the partnership as a whole.

The protocol is designed to:

- Support action in accordance with any of the legislative provisions of the Crime and Disorder Act 1998
- Govern the use and management of information provided by the parties to this agreement
- Assist with the exchange of information to support other crime reduction activities

EXCHANGING INFORMATION AND DISCLOSURE

Information Exchange

Information Exchange relates to a physical exchange of data between one or more individuals or agencies.

Advice from the Information Commissioner indicates that public authorities may exchange data, provided that:

- They have notified their intention to do so
- That the process of exchange is in accordance with the Data Protection Act, in particular the eight principles forming Part 1 of Schedule 1.
- There is a statutory or common law power to do so.

Disclosures

Disclosures of information and in particular, personal data are bound to both common and statute law in particular, but not restricted to the following:

- The Common Law Duty of Confidentiality
- The Data Protection Act 1998
- The Human Rights Act 1998

Any disclosure of personal data must have regard to both common and statute law. For example, defamation, the common law duty of confidence and the data protection principles.

Consideration should always be given to alternative powers that exist for the purposes of data disclosure:

Consent

Many of the Data Protection issues in relation to disclosure can be avoided if the consent of the individual has been sought and obtained. Consent must be freely given after the alternatives and consequences are made clear to the person from whom permission is being sought. This will be considered to be 'informed consent'.

For the purposes of this protocol, the term 'sensitive', where applied to data refers to the categories of data termed 'sensitive' within the Data Protection Act 1998.

Reasons for Information Exchange

The processing and analysis of information and where appropriate, intelligence, is essential for identifying and limiting the activities of those committing crime and disorder along with the associated problems which adversely affect community safety and the quality of life.

The exchange of appropriate information is fundamental to the success of any strategy implemented for the purposes of reducing crime and disorder.

The opportunities for information exchange therefore:

- Assist strategic and tactical planning to disrupt crime.
- Assist Crime and Disorder partnerships to implement the provisions of the Crime and Disorder Act 1998 and other subsequent legislation.
- Assist agencies to exchange information where a power exists to do so, in accordance with the Data Protection Act and in accordance with Human Rights Act legislation.

Benefits of information exchange

The benefits of appropriate information exchange are:

- Better informed decision making and partnership working

- Enhanced inter-agency relationships
- Improved profiling of crime and disorder activity thus allowing a more effective targeting of resources.
- Reduction of Crime and Disorder throughout Lincolnshire.
- Effective monitoring and evaluation of all community safety initiatives

Witnesses, Victims and Complainants

Extreme care and careful consideration should be taken where the disclosure of information includes details of witnesses, victims or complainants.

The general rule is that information such as described by witnesses, victims or complainants should not be disclosed without first obtaining fully informed, specific and explicit consent from the individual concerned.

In all such cases, advice should be sought from the legal department, Information Sharing Officer and/or Data Protection Officer.

Any information disclosed must be processed securely and in accordance with Principle 7 of the Data Protection Act, the interpretation of which can be found in Part 1, Schedule 1 of the Act. Furthermore, recognition and compliance with information Security Policies shall be adhered to.

Information must therefore be stored securely and destroyed when no longer required for the purpose for which it is provided. See Appendix 1 to the Information Sharing Agreement. Information/data shall not be 'backed up' or archived on the premise that it may be of use for some undetermined purpose in the future.

An underlying principle of this protocol is that the Data Controller of an agency will always retain ownership of the personal data it discloses to another member of the Crime and Disorder Partnership in accordance with Section 115 of the Crime and Disorder Act. The identity of the originator must therefore be recorded against the relevant data.

A further underlying principle of this protocol is that any recipient or recipients of the same data extract must obtain the consent of the original data owner, in this case the Lincolnshire Police, before making a further disclosure.

RESPONSIBILITIES OF SIGNATORIES

It is the responsibility of all signatories to ensure that:

- Realistic expectations prevail from the outset.
- Professional, ethical standards are maintained.
- The Data Protection Principles are upheld.
- The information exchanged is kept secure and confidentiality is maintained as appropriate to the information's level of protective marking* as defined by the Data Controller.
**as defined by the Security Policy Framework.*
- A mechanism exists by which the flow of information can be controlled
- Appropriate staff training is provided on this protocol

- Adequate arrangements exist to test adherence to protocol

DESIGNATED OFFICERS/ MANAGEMENT CO-ORDINATION

Information exchanged under this protocol should be carried out via Designated Officers.

Signatories to the 'Information Sharing Agreement' will nominate Designated Officers to process or initiate requests for any personal information.

Persons requesting information from another agency must submit the request through a Designated Officer or agreed department.

The mechanism for the exchange of information should be recorded and contained within the 'Information Sharing Agreement', forming an appendix to this protocol, which will have been produced specifically for the exchange of defined data between agencies for a specified purpose.

INFORMATION SECURITY

ISO 27001 provides a baseline standard for security arrangements, which is a requirement of Principle 7 of the Data Protection Act and to which all agencies should implement.

Notwithstanding the provisions of this protocol, each request for information will be considered on a case-by-case basis with specific regard to data security.

Specific information will be required on the Information Sharing Agreement

Security – General

It is essential that the participating agencies provide personal or other sensitive information only to specific individuals authorised to receive it. The transfer, use, storage and retention of the information by each participating agency must comply both with the Data Protection Act, and with the security requirements of the agencies that have provided the information.

The following sections outline a number of procedures, adherence with which is necessary in order to meet legislative requirements and to reduce the risk of harm that might result from loss or theft of personal or other sensitive information processed as part of the agreement.

Individuals working within the YOS are also obliged to meet the security requirements of the agencies by which they are employed.

IT Security Requirements for Police Provided Information.

Personal or sensitive information must not be transferred by e-mail unless the recipient's e-mail address contains '.cjsm.net', '.pnn', '.gse', '.gsx', '.gsi' or '.nhs.net.'

Where this is the case, only information that is sensitive up to the level of 'RESTRICTED' may be e-mailed

Computers must employ unique user accounts, whose use is auditable to the extent that transactions may be identified to specific individuals, machines, times and dates.

Computer passwords must be difficult to guess, must not be disseminated to anyone, and must not be recorded in any format. They should also be changed on a regular basis or in response to any potential situation in which they may have been compromised

When leaving computers for short periods, users must activate secure screen-locks or log off from the password protected application or account that contains personal or sensitive information. When leaving their computers for longer periods or when leaving the premises, users should close down their computers.

When displaying Police Information computer screens must be angled so that their contents cannot be easily viewed through windows or open doorways. If this is not possible semi-opaque film or blinds should be used at windows.

Access to the information should be restricted to users who have the authority to see such information.

Computers must not be capable of connecting to 3rd party networks used by different agencies within premises unless a specific agreement to do so has been reached between the security and IT personnel of the relevant agencies.

Any personal or other sensitive information that is transferred onto floppy disks, CDs or other removable media, must be clearly labelled and stored securely when not in use. These media must be securely disposed of when no longer required.

Printers must be located within sight of the computers to which they are attached. They must not be left unattended when printing out personal or other sensitive information. Printouts must be removed from printers immediately after printing and must be stored securely when not in use.

Physical Security Requirements for Police Provided Information

Lockable containers must be provided, with restricted access, in which they must store hard-copy Police information when it is not in use.

Once a paper document is no longer required, it must either be securely returned to the agency that provided it, or destroyed in a paper shredder with a cross-shredding facility that has been installed within the recipients premises.

Documents waiting to be destroyed must be stored securely.

All authorised users are responsible for preventing unauthorised access to non-public areas of the premises. Personal or sensitive information on computer screens or in hard-copy format must not be accessible to non-authorised individuals such as cleaning or maintenance personnel or visitors to premises.

Police information must be kept out of sight of unauthorised, prying eyes. e.g. Contractors, visitors, cleaners, etc

Records, in any format, that contain personal or other sensitive information must not be removed from recipient's premises without the agreement of the agency that provided the information.

Information taken from premises must be kept secure at all times, must not be made available to individuals who are not authorised to see it, and must only be used for the purposes specified within the 'Information Sharing Agreement'.

Personnel Security

Each participating agency is responsible for ensuring that reasonable efforts have been made to establish the trustworthiness and integrity of the individuals that process personal and other sensitive information covered by the terms of this protocol. These individuals must be made clearly aware of the requirement for them to process personal and other sensitive information securely, in compliance with the relevant legislation, and only for the purposes prescribed by this document.

Where it is found that an individual, who carries out work involving the processing of personal or other sensitive information covered by the terms of this protocol, poses an unacceptable risk to the work, his or her involvement in this work must be terminated by his or her employing agency.

Information Breaches

Complaints and breaches to this protocol should be dealt with by utilising any established agency policies and procedures for breaches and complaints made in relation to appropriate legislation in connection with the agreed information exchange and data processing.

Any disclosure of information by an employee, which is done in bad faith or for motives for personal gain, will be the subject of an investigation and be treated as a serious matter. 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.

All agencies are reminded of the Data Protection Act Principles and Section 55 and Section 61 Offences.

It is the responsibility of all parties to notify the other party of any known breach or infringement immediately and remedial action must be agreed and actioned by all relevant agencies concerned.

Major breaches may result in this protocol being temporarily suspended or withdrawn completely.

Subject Access

Subject Access is an individuals right to have a copy of information relating to them which is processed by an organisation.

If an agency or recipient receives a Subject Access Request and the personal data is identified as belonging to another agency or data controller, it will be the responsibility of the recipient to contact the data controller of the agency, usually the Data Protection Officer who will take the lead as far as the request is concerned. Communication must take place speedily thus allowing the servicing of the request to take place within the Statutory 40 calendar day, time period.

Confidentiality Agreement

(to be read by all members of staff having access to the data)

The information exchanges will only be used for the purpose for which it was requested and it will be securely stored and destroyed when no longer required. Any agency and its employees becoming recipients for the purpose of this information exchange process will, upon signing this protocol, be bound by its terms and conditions.

Members of Crime and Disorder Reduction Partnerships may be requested to sign further confidentiality agreements depending upon the nature of the information provided.

VETTING

Non-Police Personnel Vetting relates to the vetting of persons other than police personnel, who require access to police premises or police information systems. They include, for example, Volunteers, Interpreters, Crime & Disorder partners, HM Customs & Excise, Department of Works & Pensions, Work Experience, Lay Visitors and a variety of contractors and volunteers, some of whom require full access to our IT systems or to sensitive police information.

The purpose of vetting is to provide a standard level of protection of both government and police assets.

All non-police personnel requiring such access will be required to submit a personal information document giving consent for the vetting checks to be undertaken. The individual will be checked on the information supplied against the following databases (spent convictions are to be included):

- Criminal Records
- Police Intelligence
- Special Branch
- Professional Standards
- National Government (where applicable)
- Financial (where applicable)

The Lincolnshire Police Vetting Unit will undertake these checks.

DISCLAIMER

The Information Provider (Data Controller) disclaims all liability to the data recipient in connection with the data recipient's use of data supplied under this agreement and shall not, under any circumstances, be responsible for any special, indirect or consequential loss or damages including but not limited to loss of profits arising from the use of the data by the data recipient.

INDEMNITY

The data recipient shall indemnify the Information Provider in full in respect of any loss or damage caused to the Information Provider as a consequence of the unauthorised disclosure of data supplied under this agreement.

REVIEWS

This protocol and any appendices will be reviewed within 6 months of initial signing and then at least annually, or sooner if required, at the instigation of the Force Information Manager for the Lincolnshire Police or any Designated Officers.

SIGNATURES

For the purposes of working together in partnership in accordance with the Crime and Disorder Act 1998, we agree to work in accordance with the provisions of this protocol and attached processing documentation.

DATA CONTROLLER (or on behalf of)

Organisation: Lincolnshire Police.....

Signature:

Name, Position/Rank:

Date:

RECIPIENT (or on behalf of)

Organisation:

Signature:

Name, Position/Rank:

Date:

**TWO COPIES OF THIS DOCUMENT SHOULD BE SIGNED.
ONE TO BE RETAINED BY LINCOLNSHIRE POLICE, THE OTHER TO BE RETAINED BY
THE PARTNER AGENCY/ORGANISATION**