PREFACE

This high level document has been jointly developed by public sector organisations in Leicestershire, Leicester and Rutland to facilitate the sharing of information amongst key organisations.

This Information Sharing Protocol has been developed following consultation and working experience over a period of over 10 years by participating bodies, chiefly public authorities such as the Police, Health and Local Authorities. This protocol previous versions were agreed and implemented across the City of Leicester and County of Leicestershire. This protocol supercedes all previous versions.
1. **INTRODUCTION**

1.1 This document is an Information Sharing Protocol (for the purpose of this protocol, the terms data and information are synonymous). The aim of this document is to facilitate sharing of all personal, sensitive and non-personal data between the public, private and voluntary sectors so that members of the public receive the services they need.

1.2 Organisations involved in providing services to the public have a legal responsibility to ensure that their use of personal data is lawful, properly controlled and that an individual’s rights are respected. This balance between the need to share personal data to provide quality service and protection of confidentiality is often a difficult one to achieve.

1.3 The legal situation regarding the protection and use of personal data can be unclear. This situation may lead to information not being readily available to those who have a genuine need to know in order for them to do their job properly. See Appendix B for Relevant Legislation.

1.4 There are fewer constraints on the sharing of non-personal data, that is data which either does not identify a living individual or when combined with other information that is in or may come into the organisation’s possession will not identify a living individual.

1.5 Each partner to this protocol should ensure that all of their staff who are affected by it are

- aware of its contents and
- the obligations it and any information sharing agreements (ISA) which are created between the organisation signed up to it bring to them.

1.6 Each partner should also ensure that revisions to the protocol and ISA raised in it are signed in good time, which should be before any sharing takes place.
2. SCOPE

2.1 This overarching protocol sets out the principles for information sharing between Partner Organisations (Appendix A).

2.2 This protocol sets out the rules that all people working for or with the Partner Organisations must follow when using and sharing information.

2.3 This protocol applies to all information shared by Partner Organisations. Sharing is **not** restricted solely to information classified as Personal Data by the Data Protection Act 1998. This includes the following information:

   a) All information processed by the organisations including electronically (e.g. computer systems, CCTV, Audio etc), or in manual records;

   b) Anonymised, including aggregated data. The considerations, though less stringent, must take into account factors such as commercial or business, sensitive data, and the effect of many data sets being applied.

2.4 This Protocol will be further extended to include other public sector, private and voluntary organisations working in Partnership to deliver services.

2.5 The specific purpose for use and sharing information will be defined in the Information Agreements that will be specific to the Partner Organisations sharing information.
3. AIMS AND OBJECTIVES

3.1 The aim of this protocol is to provide a framework for the Partner Organisations and to establish and regulate working practices between Partner Organisations. The protocol also provides guidance to ensure the secure transfer of information, and that information shared is for justifiable legal purposes (see 6.3 and 11.5).

3.2 These aims include:

- To guide Partner Organisations on how to share personal information lawfully.
- To explain the security and confidentiality laws and principles of information sharing.
- To increase awareness and understanding of the key issues.
- To emphasise the need to develop and use Information Sharing Agreements.
- To support a process that will monitor and review all information flows.
- To encourage flows of information.
- To protect the Partner Organisations from accusations of wrongful use of personal data.
- To identify the legal basis for information sharing.

3.3 By becoming a Partner to this Protocol, Partner Organisations are making a commitment to:

- Apply the Information Commissioner’s Code of Practice’s ‘Fair Processing’ and ‘Best Practices’ Standards;
- Adhere to or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act 1998; (See Appendix B).
- Develop local Information Sharing Agreements (ISA) that specify transaction details. (See Appendix E for template).

3.4 Partner Organisations are expected to promote staff awareness of the major requirements of Information Sharing. This will be supported by the production of appropriate guidelines where required that will be made available to all staff via the Partners’ Intranet sites and/or via other communication media.
4. **THE LEGAL FRAMEWORK**

4.1 The principal legislation concerning the protection and use of personal information is listed below and further explained in Appendix B:

- Human Rights Act 1998 (article 8)
- The Freedom of Information Act 2000
- Data Protection Act 1998
- The Common Law Duty of Confidence
- Computer Misuse Act
- Civil Contingencies Act 2004

4.2 Other legislation may be relevant when sharing specific information.

4.3 As part of each ISA, Partner Organisations should identify how they will meet its legal obligations and the legal basis (legislation and appropriate section(s)) under which information may be shared.
5. INFORMATION COVERED BY THIS PROTOCOL

5.1 All Information, including personal data and sensitive personal data as defined in the Data Protection Act 1998 (DPA). In order to reduce the risks of DPA compliance and security breaches where possible anonymised data should be used.

5.2 Personal Data

5.2.1 The term ‘personal data’ refers to any data held as either manual or electronic records, or records held by means of audio and/or visual technology, about an individual who can be personally identified from that data.

5.2.2 The term is further defined in the DPA as:

- Data relating to a living individual who can be identified from those data;
- Any other information which is in the possession of, or is likely to come into the possession of the data controller (person or organisation collecting that information).

5.2.3 The DPA also defines certain classes of personal information as ‘sensitive data’ where additional conditions must be met for that information to be used and disclosed lawfully.

5.2.4 An individual may consider certain information about themselves to be particularly private and may request other data items to be kept especially confidential e.g. any use of a pseudonym where their true identity needs to be withheld to protect them.

5.3 Anonymised Data

5.3.1 Organisations should ensure anonymised data, especially when combined with other information from different agencies, does not identify an individual, either directly or by summation.

5.3.2 Anonymised data about an individual can be shared without consent (subject to certain restrictions regarding health/social care records), in a form where the identity of the individual cannot be recognised i.e. when:

- Reference to any data item that could lead to an individual being identified has been removed;
- The data cannot be combined with any data sources held by a Partner to produce personal identifiable data.
6. RESPONSIBILITIES WHEN SHARING INFORMATION

6.1 General

Each Partner Organisation is responsible for ensuring that their organisational and security measures protect the lawful use of information shared under this Protocol.

6.1.1 Partner Organisations will ensure a reasonable level of security for supplied information, personal or non-personal, and process the information accordingly.

6.1.2 Partner Organisations accept responsibility for independently or jointly auditing compliance with the Information Sharing Agreements in which they are involved within reasonable time-scales.

6.1.3 Every organisation should consider making it a condition of employment that employees will abide by their rules and policies in relation to the protection and use of confidential information. This condition should be written into employment contracts and any failure by an individual to follow the policy should be dealt with in accordance with that organisation’s disciplinary procedures.

6.1.4 Every organisation should ensure that their contracts with external service providers include a condition that they abide by their rules and policies in relation to the protection and use of confidential information.

6.1.5 The Partner Organisation originally supplying the information should be notified of any breach of confidentiality or incident involving a risk or breach of the security of information.

6.1.6 Partner Organisations should have a written policy for retention and disposal of information.

6.1.7 Partner Organisations must be aware that a data subject may withdraw consent to processing (i.e. Section 10 DPA) of their personal information. In this case processing can only continue where an applicable Data Protection Act Schedule 2, and if relevant Schedule 3, purpose applies.

6.1.8 Where the Partner Organisations rely on consent as the condition for processing personal data then withdrawal means that the condition for processing will no longer apply. Withdrawal of consent should be communicated to Partner Organisations and processing cease as soon as possible.
6.2 **Personal Data**

Personal data should only be shared for a specific lawful purpose or where appropriate consent has been obtained.

6.2.1 Staff should only be given access to personal data where there is a legal right, in order for them to perform their duties in connection with the services they are there to deliver.

6.2.3 This agreement does not give licence for unrestricted access to information another Partner Organisation may hold. It sets out the parameters for the safe and secure sharing of information for a justifiable need to know purpose.

6.2.4 Each signatory organisation to an ISA is responsible for ensuring every member of its staff is aware and complies with the obligation to protect confidentiality and a duty to disclose information only to those who have a right to see it.

6.2.5 Each signatory organisation should ensure that any of its staff accessing information under an ISA is trained and fully aware of their responsibilities to maintain the security and confidentiality of personal information.

6.2.6 Each signatory organisation should ensure that any of its staff accessing information under an ISA to follow the procedures and standards that have been agreed and incorporated within this Information Sharing Protocol and any associated Information Sharing Agreements.

6.2.7 Each Partner Organisation will share information in compliance with the principles set out at section 4 and any other obligations detailed in both the ISP and relevant ISA.

6.2.8 Personal data shall not be transferred to a country or territory outside the EEA without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

6.3 **Non-Personal Data**

6.3.1 Partner Organisations should not assume the non-personal information is not sensitive and can be freely shared. This may not be the case and the partner from whom the information originated from should be contacted before any further sharing takes place.
7. RESTRICTIONS ON USE OF INFORMATION SHARED

7.1 All shared information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in the relevant Information Sharing Agreement unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Therefore any further uses made of this data will not be lawful or covered by the ISA.

7.2 Restrictions may also apply to any further use of non-personal information, such as commercial sensitivity or prejudice to others caused by the information’s release, and this should be considered when considering secondary use for non-personal information. If in doubt the information’s original owner should be consulted.

7.3 Additional Statutory restrictions apply to the disclosure of certain information for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection etc. Information about these will be included in the relevant ISA.
8. CONSENT – APPLIES TO PERSONAL DATA ONLY

8.1 Consent is not the only means by which personal data can be disclosed. Under the Data Protection Act 1998 in order to disclose personal data at least one condition in schedule two must be met. In order to disclose sensitive personal data at least one condition in both schedules two and three must be met. See Appendix B and Glossary for explanation (Appendix C).

8.2 Where a Partner Organisation has a statutory obligation to disclose personal data then the consent of the data subject is not required; but the data subject should be informed that such an obligation exists.

8.3 If a Partner Organisation decides not to disclose some or all of the personal data, the requesting authority must be informed. For example the Partner Organisation may be relying on a lawful exemption from disclosure or on the inability to obtain consent from the data subject.

8.4 Consent has to be signified by some communication between the organisation and the Data Subject. If the Data Subject does not respond this cannot be assumed as implied consent. When using sensitive data, explicit consent must be obtained subject to any existing exemptions. In such cases the data subject’s consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose for processing.

8.5 If consent is used as a form of justification for disclosure, the data subject must have the right to withdraw consent at any time.

8.6 Specific procedures will apply where the data subject is either not considered able to give informed consent itself because of either the data subject’s age (Gillick Competency) or where the data subject has a condition which means the data subject does not have the capacity to give informed consent. In these circumstances the relevant policy of the Partner Organisation should be referred to.
9. INDEMNITY

9.1 Each partner organisation will keep each of the other partners fully indemnified against any and all costs, expenses and claims arising out of any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its sub-contractors, employees, agents or any other person within the control of the offending partner of any personal data obtained in connection with this agreement.

10. SECURITY

10.1 It is assumed that each Partner Organisation has achieved or will be working towards ISO 27001, the International Standard for Information Security Management, compliance or a similar level of compatible security. Partner Organisations should ensure that the minimum standards of security, that they require, are agreed with Partner Organisations with whom their information will be shared and included in the ISA. This should take account of the security classification of the information.

10.2 It is accepted that not all Partners will have security classification in place. Where this is the case guidance is available for Partners at Appendix G.

10.3 Each partner signing this protocol and any individual signing the confidentiality agreement, see Appendix D, agrees to adhere to the agreed standards of security. If there is a security breach in which information received from another party under this ISA is compromised, the originator will be notified at the earliest opportunity via the postholder identified at 3.2 of the ISA, see Appendix E, who must forward details to the Information Security Section.

10.4 Where a partner has regular, specific security requirements, for example a corporate policy, either these or, if available, a hypertext link to the protocol should be included in Appendix G. This should help to avoid reviewing standards agreed previously when each new ISA is set up.

10.5 Security requirements will not be included in individual Information Sharing Agreements except where they are unique to that Agreement. This will ensure requirements are kept current, as notified, and avoid errors arising from having more than one copy of a Partner’s standard requirements.
11. INFORMATION QUALITY

11.1 Information quality needs to be of a standard fit for the purpose information is to be used for, including being complete, accurate and as up to date as required for the purposes for which it is being shared. Without this any decision made on the information may be flawed and inappropriate actions may result. Partner Organisations are expected to ensure that the Personal Data and Sensitive Personal Data that it holds is processed in accordance with DPA principles: this includes ensuring that the Data is accurate, complete and up-to-date and is not kept any longer than is necessary.

11.2 Where Partner Organisations share information under this Protocol it is expected that Partner Organisations will either have an Information Quality Strategy and the supporting processes and procedures in place or be formally working towards this.

11.3 All Partner Organisations are expected to give undertakings that information meets a reasonable quality level for the proposed purposes for which it is being shared and be able to evidence this.

11.4 It is expected that all partner organisations will have or be working towards an organisational Information Quality Strategy. In generating and maintaining this policy due regard should be paid to the Information Quality Assurance Strategy and associated supporting documents issued from time to time by the Leicestershire Information Management Advisory Group (IMAG).

11.5 Audit

Where a partner requires the ability to audit a Partner Organisation’s Information Quality standards, for example as part of a Local Area Agreement (LAA) in which the receiving partner is the lead LAA partner, this and the obligations on the partners should be identified in the contract or ISA relevant to the sharing.

12. TRAINING

12.1 All Partner Organisations staff processing information shared under this Protocol and its associated ISA are expected to be trained to a level that enables them to undertake their duties confidently, efficiently and lawfully. This is an obligation on each Partner Organisation and responsibility for it cannot be assigned to another organisation, although delivery of training can with that third party’s consent.

12.2 To minimise the costs associated with training and to ensure that all staff participating in activities based on information shared under a specific ISA it is strongly advised that partners collaborate in the development and delivery of training. Obligations and costs arising out of such collaborative working should be clearly identified in the ISA.
12.3 For the avoidance of doubt, where collaborative training is not adopted this should be stated in the ISA.
13. INDIVIDUAL RESPONSIBILITIES

13.1 Every individual working for the organisations listed in this Partnership Agreement is personally responsible for the safekeeping of any information they obtain, handle, use and disclose.

13.2 Every individual should know how to obtain, use and share information they legitimately need to do their job.

13.3 Every individual has an obligation to request proof of identity, or takes steps to validate the authorisation of another before disclosing any information requested under this protocol and associated ISA’s.

13.4 Every individual should uphold the general principles of confidentiality, follow the guidelines set out in this Protocol and seek advice when necessary.

13.5 Every individual should be aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal. Criminal proceedings might also be brought against that individual.

14. GENERAL PRINCIPLES

14.1 The principles outlined in this protocol are recommended good standards of practice or legal requirements that should be adhered to by all Partner Organisations.

14.2 This protocol sets the core standards applicable to all Partner Organisations and should form the basis of all Information Sharing Agreements established to secure the flow of personal information.

14.3 This protocol should be used in conjunction with local service level agreements, contracts or any other formal agreements that exist between the Partner Organisations.

14.4 All parties signed up to this protocol are responsible for ensuring that organisational measures are in place to protect the security and integrity of personal information and that their staff are properly trained to understand their responsibilities and comply with the law.

14.5 This protocol has been written to set out clear and consistent principles that satisfy the requirements of the law that all staff must follow when using and sharing personal information.

14.6 The specific purpose for use and sharing information will be defined in the Information Sharing Agreements that will be specific to the Partner Organisations sharing information.
15. REVIEW ARRANGEMENTS

15.1 This overarching agreement will be formally reviewed annually by IMAG and the Leicester Partnership Information Group, unless new or revised legislation or national guidance necessitates an earlier review.

15.2 Any of the signatories can request an extraordinary review at any time where a joint discussion or decision is necessary to address local service developments.
APPENDIX A - SIGNATURES AND CONTACT INFORMATION

Agreement: We the undersigned do hereby agree to implement the terms and conditions of this Protocol.

Contact Information

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Chief Executive/Officer</th>
<th>Signature</th>
<th>Date</th>
<th>Contact Name</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B – RELEVANT LEGISLATION

THE DATA PROTECTION ACT 1998

Data Protection legislation governs the standards for the processing of personal data including the collection, use of and disclosure of such data. The legislation requires that data controllers meet certain obligations. It also give individuals or ‘data subjects’ certain rights with regard to their own personal data. The main standard for processing personal data is compliance with the eight data protection principles summarised as follows:

i) All personal data will be obtained and processed fairly and lawfully.

ii) Personal data will be held only for the purposes specified.

iii) Only personal data will be held which are adequate, relevant and not excessive in relation to the purpose for which the data are held.

iv) Steps will be taken to ensure that personal data are accurate and where necessary, kept up to date.

v) Personal data will be held for no longer than is necessary.

vi) Individuals will be allowed access to information held about them and, where appropriate, permitted to correct or erase it.

vii) Procedures will be implemented to put in place security measures to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of, information.

viii) Personal data shall not be transferred to countries outside the European Economic area except in limited circumstances.

The most significant principle is the first principle which states that personal data shall be processed fairly and lawfully and shall not be processed unless at least one Schedule 2 condition and in the case of ‘sensitive personal data’, at least one Schedule 3 condition is also met.

The type of information being disclosed for the purposes of this exchange agreement will almost always be ‘sensitive personal data’ which means that at least one of both Schedule 2 and Schedule 3 conditions must be satisfied.

Even in the event that the prevention and detection of crime exemption (Section 29 Data Protection Act) is being relied upon, or other power such as S.115 Crime and Disorder Act, Schedules 2 and 3 conditions must still be satisfied.

The first Data Protection Principle requires the data controller to process personal data fairly and lawfully. All information processed under this protocol, and any and all associated information sharing agreements, must be processed lawfully.
Data Protection Act 1998 (Principle 1) Schedules 2 and 3.

The most relevant schedules are:

- The processing is however likely to be necessary for compliance with any legal obligation, such as the Police Acts and the Local Government Act 2000.

- It is likely that the most relevant condition will be that the processing is necessary for the exercise of any other functions of a public nature exercised in the public interest by any person.

- The legitimate interests condition may be appropriate, but cases are likely to arise whereby a service user could clearly challenge this depending upon the circumstances.

The most relevant conditions in Schedule 3 are s3 and s7.

Section 3. The processing is necessary

(a) in order to protect the vital interests of the data subject, or another person, in a case where:
   (i) consent cannot be given by, or
   (ii) on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject, or
   (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Section 7. (1) Processing is necessary:

(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under an enactment.

Although the aforementioned conditions are likely to apply to any or all of the variable circumstances, it is likely that for the purposes of this exchange agreement one of the additional conditions specified in secondary legislation (Processing of Sensitive Data Order 2000) may also apply:

Data Protection (Processing of Sensitive Personal Data) Order 2000/417

The Order lists additional circumstances in which sensitive personal data may be processed. For example, it covers processing for the purposes of the prevention or detection of any unlawful act, where seeking the consent of the data subject would prejudice those purposes. It also covers processing required to discharge functions involving the provision of services such as confidential counselling and advice where the subject’s consent has not been obtained.

In each of the examples above processing would have to be “in the substantial public interest”. This could mean, for example, that processing is necessary to protect public safety or to protect vulnerable people.
THE HUMAN RIGHTS ACT 1998

The UK Human Rights Act 1998 gives further effect in domestic law to Articles of the European Convention on Human Rights (ECHR). The Act requires all domestic law be compatible with the Convention Articles and places a legal obligation on all public authorities to act in a manner compatible with the convention. Should a public authority fail to act in such a manner then legal action can be taken under Section 7 of the Act.

Article 8 of the Act states that:

“Everyone has the right to respect for his private and family life, his home and his correspondence and that there shall be no interference by a public authority with this right except as in accordance with the law”. As this exchange of information will be for the purposes of one of the following legitimate aims:

- In the interests of national security.
- Public Safety.
- Economic well being of the country.
- The prevention of crime and disorder.
- The protection of health or morals.
- The protection of the rights or freedoms of others.

FREEDOM OF INFORMATION ACT 2000

Information held by or on behalf of a public authority may be disclosed to a party requesting it except where a statutory exemption applies. For example, personal data is normally exempt under the Act (but may be disclosable under DPA 1998); as is information provided under a duty of confidence.

LOCAL GOVERNMENT

The main power specific to local authorities is section 2 Local Government Act 2000 - the power of "well-being". This enables LA's to do "anything" to promote social, economic, or social well-being in their area provided the act is not specifically forbidden by other statute (including the Data Protection Act) and that in carrying out the act it gives regard to its own community strategy. For example, all councils are taking measures, including data sharing, to reduce crime in its area in order to promote well-being. In addition S111 Local Government Act 1972 enables local authorities to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place. The above are general powers available to local authorities. In addition, authorities are granted statutory powers relating to specific activities and these should be referred to as appropriate in the Information Exchange Agreement.
CIVIL CONTINGENCIES ACT 2004

In emergencies it may be in the interests of affected people who are most vulnerable for personal data to be shared with emergency responders. Sharing personal information will assist emergency responders to perform their statutory duties.

The Civil Contingencies Act 2004 1(1) defines an emergency as “an event or situation which threatens serious damage to human welfare and/or the environment or war or terrorism which threatens damage to security”.

Guidance on Part 1 of the Civil Contingency Act 2004 defines vulnerable people as those “that are less able to help themselves in the circumstances of an emergency”. Groups considered to be most vulnerable in emergencies include the following: children, older people, mobility impaired, mental/cognitive functions impaired, sensory impaired, individuals supported by health or local authorities, temporarily or permanently Ill, individuals cared for by relatives, homeless, pregnant women, minority language speakers, tourists, travelling community.

The principles and legislative provisions related to information sharing apply to the planning, response and recovery phases of emergencies.

Statutory guidance sets out the responsibilities on Category 1 responders (with the co-operation of Category 2 responders) to plan for and meet the needs of those who may be vulnerable in emergencies.

This includes:

- Making and maintaining plans for reducing, controlling or mitigating the effects of any emergency.
- Warning and informing.
- Business continuity.

Category 1 responders are those organisations at the core of emergency response (e.g. emergency services, local authorities). Category 1 responders are subject to the full set of civil protection duties. They are required to:

- Assess the risk of emergencies occurring and use this to inform contingency planning;
- Put in place emergency plans;
- Put in place Business Continuity Management arrangements;
- Put in place arrangements to make information available to the public about civil protection matters and maintain arrangements to warn, inform and advise the public in the event of an emergency;
- Share information with other local responders to enhance co-ordination;
- Co-operate with other local responders to enhance co-ordination and efficiency; and
- Provide advice and assistance to businesses and voluntary organisations about business continuity management (Local Authorities only).

The Data Protection Act 1998 Schedule 2(4) and 6(1) and Schedule 3(3) and 3(4).

In an emergency the sharing of personal information may be necessary to protect the affected person’s vital interests. The information to be shared will be determined by the nature of the emergency. For example if there is a need to evacuate people from their homes, knowledge of where people with special needs are located would enable speedy application of appropriate assistance.

Sharing information is also necessary for responders to fulfil statutory functions, and to perform public functions in the public interest in relation to the required response to emergency incidents. Additionally, in emergencies the sharing of personal information categorised as “sensitive” is necessary to protect vulnerable persons’ vital interests and to perform statutory functions.
POLICE ACT 1996

The Police Act 1996 gives a Constable certain powers. Section 30(1) gives constables all the powers and privileges of a constable throughout England and Wales and Section 30(5) defines these powers as powers under any enactment when ever passed or made. These powers include the investigation and detection of crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.

In addition, the Code of Practice on the Management of Police Information 2005 defines the policing purpose as:-
• protecting life and property,
• preserving order,
• preventing the commission of offences,
• bringing offenders to justice,
• any duty or responsibility arising from common or statute law

The policing purpose set out in the Code does not replace or supersede any existing duty or power defined by statute or common law. In addition, this does not define every policing activity and does not mean that there is no legal basis for performing such activities. For example, roads policing, public order, counter-terrorism or protection of children or other vulnerable groups while not referred to explicitly are nonetheless legitimate policing functions.

THE CRIME AND DISORDER ACT 1998

Section 115 of the Crime and Disorder Act 1998 confers a power on any ‘relevant authority’ (which are the police, local authority, health authority and probation service or to any other person acting on behalf of such authority) to exchange that information which is ‘necessary’ or ‘expedient’ to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder. The parties to this exchange agreement are relevant authorities for the purposes of this legislation.

Section 17 Crime and Disorder Act 1998 requires that all Local Authorities consider crime and disorder reduction while exercising their duties. Sections 5 and 6 of the Crime and Disorder Act imposes a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area.

COMMON LAW DUTY OF CONFIDENTIALITY

The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are generally three categories of exception to the duty of confidence:
• Where there is a legal compulsion to disclose.
• Where there is an overriding duty to the public.
• Where the individual to whom the information relates consented.
Partners should consider which of these conditions are the most relevant ones for the purposes of an agreement. The guidance from the Information Commissioner states that because such decisions to disclose ‘in the public interest’ involves the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking those decisions. The partners to this agreement should document within this agreement how this duty will be maintained, e.g. need to know,
APPENDIX C - GLOSSARY OF TERMS

Accessible Record – unstructured personal information usually in manual form relating to health, education, social work and housing.

Agent – Person who acts on behalf of another.

Aggregated – collated information in a tabular format.

Anonymised data – Anonymised data is Personal Data or Sensitive Personal Data that has been redacted so as to exclude personal information. If the Data Controller has information, which allows the Data Subject to be identified, regardless of whether or not they intend to identify the individual is immaterial - in the eyes of the IC this is not anonymous data. Data Controller must be able to justify why and how the data is no longer personal.

CCTV – close circuit television.

Consent – The Information Commissioner’s legal guidance to the Data Protection Act 1998 is to refer to the Directive, which defines consent 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” (3.1.5).

Data/Information –
   a) Information being processed by means of equipment operating automatically or
   b) Information recorded with the intention it be processed by such equipment.
   c) Recorded as part of a relevant filing system or
   d) Not in a or b or c, but forming part of an accessible record.

Data Controller – a person or a legal body such as a business or public authority who jointly or alone determines the purposes for which personal data is processed.

Data Flows – the movement of information internally and externally, both within and between organisations.

Data Processing – any operation performed on data. The main examples are collection, retention, deletion, use and disclose.

Data Processor – operates on behalf of the Data Controller. Not staff.

Data Set – a defined group of information

Data Subject – an individual who is the subject of personal information.

Disclosure – the passing of information from the Data Controller to another organisation / individual

Duty of Confidentiality – everyone has a duty under common law to safeguard personal information.

European Economic Area (EEA) – this consists of the EU members together with Iceland, Liechtenstein and Norway.
Appendix C: Glossary of Terms Continued…

**Fair processing** – to inform the Data Subject how the data is to be processed before processing occurs.

**Health Professional** – In the Data Protection Act 1998 "health professional" means any of the following who is registered as:

A medical practitioner, dentist, optician, pharmaceutical chemist, nurse, midwife or health visitor, and osteopaths.

and

Any person who is registered as a member of a profession to which the Professions Supplementary to Medicine Act 1960 currently extends to, clinical psychologists, child psychotherapists and speech therapist, music therapist employed by a health service body, and scientist employed by such a body as head of department.

**Health Record** – any information relating to health, produced by a health professional.

**Information Exchange** – the ad hoc exchange of information between two or more parties to achieve specific operational requirements that by its nature is variable and infrequent. In this case an ISA is not appropriate.

**Information Sharing Agreement** – the local information sharing agreement based on the attached template Appendix E.

**Need to know** – to access and supply the minimum amount of information required for the defined purpose.

**Personal Data** – means data relating to a living individual who can be identified from those data (including opinion and expression of intention).

**Processing** – any operation performed on data. Main examples are collect, retain, use, disclosure and deletion.

**Purpose** – the use / reason for which information is stored or processed.

**Recipient** – anyone who receives personal information.

**Relevant Filing System** – two levels of structure, (i) filing system structured by some criteria (ii) each file structured so that particular information is readily accessible.

**Sensitive Personal Data** – data concerning racial origin, politics, Trade Union activity, health, sexuality, offending etc.
Appendix C: Glossary of Terms Continued…

**Serious Crime** – There is no absolute definition of "serious" crime, but section 116 of the Police and Criminal Evidence Act 1984 identifies some "serious arrest-able offences".

These include:

- Treason
- Murder
- Manslaughter
- Rape
- Kidnapping
- Certain sexual offences
- Causing an explosion
- Certain firearms offences
- Taking of hostages
- Hijacking
- Causing death by reckless driving
- Offences under prevention of terrorism legislation (disclosures now covered by the Prevention of Terrorism Act 1989).

**Subject Access** – the individual’s right to obtain a copy of information held about themselves.

**Third Party** – any person who is not the data subject, the data controller, the data processor (includes Health, Housing, Education, Carers, Voluntary Sector etc. as well as members of the public).
APPENDIX D - CONFIDENTIALITY STATEMENT

To enable the exchange of information between attendees at this meeting to be carried out in accordance with the Data Protection Act 1998, the Human Rights Act 1998 and the common law duty of confidentiality, all attendees are asked to agree to the following. This agreement will be recorded in the minutes.

1. Information can be exchanged within this meeting for the purpose of identifying any action that can be taken by any of the agencies or departments attending this meeting to resolve the problem under discussion.

2. A disclosure of information outside the meeting, beyond that agreed at the meeting, will be considered a breach of the subjects’ confidentiality and a breach of the confidentiality of the agencies involved.

3. All documents exchanged should be marked ‘Restricted – not to be disclosed without consent’. All minutes, documents and notes of disclosed information should be kept in a secure location to prevent unauthorised access.

4. If further action is identified, the agency(ies) who will proceed with this action(s) should then make formal requests to any other agencies holding such personal information as may be required to progress this action quoting their legal basis for requesting such information. Information exchanged during the course of this meeting must not be used for such action.

5. If the consent to disclose is felt to be urgent, permission should be sought from the Chair of the meeting and a decision will be made on the lawfulness of the disclosure such as the prevention or detection of crime, apprehension or prosecution of offenders, or where it is required to prevent injury or damage to the health of any person.

This confidentiality agreement is in relation to the
........................................................................................................................................meeting(s)

Signature........................................................................................................Date...........................

Name..........................................................................................................................

Representing...(Name and/or Organisation)
........................................................................................................................................

Copies of this signed agreement are to be held by the Chair.
APPENDIX E - INFORMATION SHARING AGREEMENT (ISA) TEMPLATE

All wording in bold should be included in your Information Sharing Agreement and all sections need to be included. If the wording is not in bold it will give you guidance on what you will need to agree with your partners.

1. Policy Statements and Purpose of this Information Sharing Agreement

   This section should include a policy statement that should explain why there is a need to share data with each of the Partner organisation(s) and the aims and objectives that this will achieve.

2. Legal Basis for Information Sharing

   Each partner organisation should be able to identify their legal basis for sharing this data. This legal basis may come from common law, statute or legal precedent, which may be supported by Home Office guidance, professional/executive bodies, e.g. Dept of Health, Association of Chief Police Officers, Dept of Education, etc. This will enable partners to defend a challenge with regard to the Data Protection Act 1998 and/or the Human Rights Act 1998. Some relevant legislation relating to the sharing of Personal Data is listed in App B. It is not an exhaustive list. You should delete those which do not apply and add any others depending on which organisation are represented in your data exchange process.

   Each organisation should identify how it intends to comply with its obligations under:

   1) The Data Protection Act 1998;
   2) The Human Rights Act 1998; and

   Where an organisation has policies, processes and procedures in place to cover this a cross-reference to these documents will suffice.

   It is also important to ensure that any partner/individual that receives personal data and holds and processes such data is able to identify a paragraph in Schedule 2 of the Data Protection Act 1998 to ensure that the processing is fair and lawful. If the personal data is sensitive data a paragraph in Schedule 3 will also need to be identified.

   This ISA has been developed to achieve the objectives as set out in Section 1. It is the intention that all aspects of information sharing and disclosure relating to this sharing agreement shall comply with legislation that protects personal data - see Appendix B.
3. Information

3.1 What data is it necessary to share?

The personal data you share must be proportionate and should be the minimum amount needed to achieve the purpose identified in Section 1. You should decide if you could do this using information that does not identify individuals (anonymised data).

If personal data must be used, you should specify as closely as possible the details and the type of data that each partner will disclose and to which other partner, for example, client name, home address or date of birth. If forms are used to request or disclose the data, attach them as an appendix.

You may find that completing the form below will assist, alternatively you could list each partner in turn and specify what data they will share and to whom. This is to ensure that it is clear who the data controller is for each data item and that any records which are subsequently created from information exchanged under this agreement should identify the source of that data.
The data sets shown are **for example** only and you use that which applies and add any specific data sets not listed here.

<table>
<thead>
<tr>
<th>Data Set</th>
<th>Who from</th>
<th>Who to</th>
<th>Why</th>
<th>Which Organisation owns the information</th>
<th>Frequency of Sharing</th>
<th>How will information be shared</th>
<th>How long will data be held for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D.O.B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Address3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Postcode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Occupation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Type of Occupancy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethnic Origin of victim</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Further to this the .......... will share the following additional data:

- Geographical information system co-ordinates to within 200 square metres.
- Incident reference numbers
- The date that the incident was first reported
- The date of the incident

Ensure that all data items to be shared are listed with a clear ‘data definition’. All parties to the agreement should have a common understanding of the information to be provided / received.

For example: **Contact Name** = the name of the client’s carer (usually relative or family friend) who may be contacted by professional carers.
3.2 Who is going to be responsible for sharing this information and ensuring information is accurate?

Each partner should identify the post holder(s) responsible on a day-to-day basis for the information sharing along with their contact details. This person should also be responsible for the accuracy of any information shared.

3.3 How will you keep a record of what information has been shared?

The partners should document in the ISA how they will record what information has been shared.

3.4 How is this information going to be shared?

The partners should give consideration to how this information will be shared and document that process in the ISA, for example during XXX meetings, face to face contact. This must take account of the security classification of the information, for example personally identifiable information should not be sent by email.

3.5 Who will have access to this information and what may they use it for?

The ISA should identify who in the receiving agencies can have access to the information and what it can be used for.

3.6 Timescales

If there are any statutory or organisational time limits by which the information is required these should be included in the ISA.

3.7 How securely does the information need to be stored?

Standard security requirements are detailed at Appendix G. This section should only detail those security standards over and above those at Appendix G sharing Partners deem necessary for sharing to take place. If no further security requirements exist for the sharing exercise this section should state this, for example “The security standards detailed at Appendix G of the main ISP are considered adequate to meet security requirements for this sharing exercise.”

Each partner signing this ISA and any individual signing the confidentiality agreement agrees to adhere to the agreed standards of security. If there is a security breach in which data received from another party under this ISA is compromised, the originator will be notified at the earliest opportunity via the postholder identified at 3.2 who must forward details to the Information Security Section.

3.8 How long are you going to keep the data?

Each partner should agree and document in the ISA how long they are going to keep the paper based and electronic data having given consideration to the retention and disposal policy of the other partners. This information must be included for every item in the table above or, where appropriate, the complete data set.
3.9 **Further Use of Information**

This section should specify whether the Partners agree to any further use of the information and the process to be followed if a Partner wishes to use the information for purposes other than defined in this agreement.

**NB** Partner’s should not assume the non-personal information is not sensitive and can be freely shared. This may not be the case and the partner from whom the information originated from should be contacted before any further sharing takes place.

4 **Breach of confidentiality**

This section should explain the procedure the Partners will follow if there is a breach of this Agreement by a Partner or a third party who has received information under this agreement. You should include:

- How partners will be notified and which post holder should be notified in each agency.
- How this will be investigated e.g. Information Commissioner, police?
- Agree what action will be taken e.g. disciplinary action, criminal proceedings.

5 **Indemnity**

This section should contain details of any indemnity that is required for this specific information sharing exercise over and above that listed in section 11 of the main ISP.

In certain circumstances signatories may decide to amend this statement or to dispense with it, for example their insurer will not honour it. In this case the parties should clearly document what, if anything is in place, and include the subsequent risk exposure as part of the regular risk management review.

6 **Individuals who cannot be covered by the Indemnity**

The parties to this ISA understand that in keeping with Government initiatives to invite a wider spectrum of society to assist the relevant authorities to implement the Crime and Disorder Act 2000, it is likely that there will be individuals present at certain meetings who are not employed by an organisation and therefore are not in a position to sign this ISA due to the liability of the indemnity.

In order to ensure that the data controllers who are supplying personal information to the meeting fulfil their duties under Data Protection Act 1998 and that the principles are complied with, it is recommended that the first time any individual attends a meeting covered by a ISA is required to sign a confidentiality agreement as at Appendix D. The responsibility for ensuring that this takes place and for retaining the signed copies lies with the Chair of the meeting.
7 **Review of Information Sharing Agreements**

All ISA will be reviewed and subjected to a risk based audit. This section should define how and when the ISA will be reviewed and audited. It is recommended that each ISA is reviewed one year after signature and at an agreed period thereafter. The frequency will depend on a variety of things such as the volatility of the data concerned and its sensitivity. Risk Management review programs should be detailed in the ISA and include who is responsible for both undertaking them and signing them off within each organisation.

This review is the responsibility of the individuals who own the applications where the data originates from and should be carried out in consultation with the Data Protection/Information Security Section. Guidance on how to carry out the review is attached as [Appendix F](#).

8. **Closure/termination of agreement**

Any partner organisation can suspend this ISA for 45 days if security has been seriously breached. This should be in writing and be evidenced.

Any suspension will be subject to a Risk Assessment and Resolution meeting, the panel of which will be made up of the signatories of this agreement, or their nominated representative. This meeting to take place within 14 days of any suspension.

Termination of this Information Sharing Agreement should be in writing to all other Partner Organisations giving at least 30 days notice.

9 **Freedom of Information Act 2000 (FOIA)**

It is intended that each Partner Organisation (PO) shall publish this ISA on its website and refer to it within its Publication Scheme. If a PO wishes to withhold all or part of the ISA from publication it shall inform the other PO’s as soon as reasonably possible. Partner organisations shall then endeavour to reach a collective decision as to whether information is to be withheld from publication or not.

Information shall only be withheld where, should an application for that information be made under FOIA 2000 it is likely that the information would be exempt from disclosure and the public interest lie in favour of withholding. However, nothing in this paragraph shall prevent the individual Partner Organisations from exercising its obligations and responsibilities under FOIA 2000 as it sees fit.
Requests for Disclosure of Information received under this ISA

All recorded information held by public sector agencies is subject to the provisions of the Freedom of Information Act 2000 and the Data Protection Act 1998. While there is no requirement to consult with third parties under FOIA, the parties to this ISA will consult the party from whom the information originated and will consider their views to inform the decision making process.

Working Examples

Partners should document scenario where sharing of information for the purposes of the Agreement is and is not appropriate. This will better help practitioners understand the scope of the Agreement and assist in their understanding of it in their day to day work.

Joint Education

Partners to an ISA should document here their approach to training in a new ISA to ensure all staff for all participating bodies have a similar level of awareness of the ISA at inception. This should include responsibility for producing the training, responsibility for agreeing it and responsibility for delivering it, and any associated charges.

Partners should also identify how further training to cover both new starters and refresher updates will be provided.

If no collaboration is to take place on training this should be identified for the avoidance of doubt.

Information Quality

Partners should agree and document any specific information quality obligations arising under this agreement. This should include any audit requirements.

If no additional information quality requirements this should be identified for the avoidance of doubt.

Appropriate Signatories

Each Partner should identify who is the most appropriate post holder within their agency to sign the ISA having taken account of their organisational policy and the fact that the signatory must have delegated responsibility to commit their organisation to the indemnity. It is the responsibility of the individuals identified at 3.2 to ensure that copies of the ISA are made available as necessary to ensure adherence to the ISA.

I confirm that this ISA has been prepared in consultation with the DPO for each signatory.
APPENDIX F - PROCESS FOR REVIEW OF AN INFORMATION SHARING AGREEMENT

The aim of a review is to ensure that the ISA is achieving its purpose and that the actual process of exchanging data is operating efficiently.

1 Policy Statements and Purpose of this Information Sharing Agreement

Is the policy statement and the purpose as identified in the ISA still accurate in relation to the present use of the information?

2 Legal Basis for Information Sharing

Do the legal bases in the ISA cover all the parties?

3 What information is it necessary to share?

Is the information which is shared by the parties in accordance with the ISA?

4 Who is going to be responsible for sharing this information and ensuring it is accurate?

Is the contact list up to date and accurate?

5 How will you keep a record of what information has been shared?

How are the parties keeping a record of what information has been shared? Random samples of the information shared could be checked against the source record to see if there is evidence of the information sharing.

6 How is this information going to be shared?

Is information still being shared in accordance with the ISA?

7 Who will have access to this information and what may they use it for?

What use of the information is made by the parties receiving information and is access restricted in accordance with the ISA?

8 Timescales

Are any timescales in the ISA being adhered to?

9 How securely does the information need to be stored?

Are all the parties applying the security measures in accordance with the ISA – see Appendix G for applicable standards?

10 How long are you going to keep the information?

Are all the parties retaining and destroying the data in accordance with the ISA?
11 Further Use of Information

Is there any evidence that information is being used by any party for purposes other than in accordance with the ISA without consent from the originator?

12 Breach of confidentiality

Have there been any breaches of confidentiality which have not been reported to the other parties? How have any breaches been dealt with?

13 Indemnity/confidentiality agreements

Is there evidence that any individual who is not covered by an organisation which is a signatory to the ISA has signed a confidentiality agreement and are these held on behalf of the Chair?

14 Freedom of Information Act 2000 (FOIA)

Is this ISA publicly available and also available internally for relevant staff?

15 Requests for Disclosure of Information received under this ISA

Have there been any instances where a party has disclosed information received under this ISA without consulting the originating party?

16 Appropriate Signatories

Is the ISA signed by appropriate staff?

Review was carried out by:

Name …………………………………………………………………………

Signature………………………………………………………………………

Organisation……………………………………………………………………

Date………………………………………………………………………………

Name …………………………………………………………………………

Signature………………………………………………………………………

Organisation……………………………………………………………………

Date………………………………………………………………………………

A copy of this review should be stored with the ISA. Any deficiencies should be brought to the attention of the Signatories as appropriate.
APPENDIX G - INFORMATION SECURITY STANDARDS

1. All partners to this ISP agree to hold all information shared under it to applicable security standards. For the purpose of this ISP applicable security standards are defined as being “achieved or will be working towards ISO 27001, the International Standard for Information Security Management, compliance or a similar level of compatible security.”

2. Each Partner accepts that other partners are professionally competent and it is for each partner to assess its security needs and identify what is and is not needed to comply with these.

3. Where a Partner has specific security needs to comply with a specific standard or requirement, for example Caldicott, it should specify these and they will be included in this Appendix. This can be either as a pdf document or by means of a hypertext link to the specifying Partner’s site. It is then for the other partners to ensure that they take these standards into consideration when assessing their own security needs.

4. Where a Partner has specified its security needs it is for that partner:
   
i) to provide the updates needed to keep this document up to date. These should be provided at least three months before such changes are due to be effective the then Chair of the Information Management Group who will be responsible for ensuring their incorporation into this Protocol; and

   ii) to confirm as part of its review process that nothing has changed to the then reviewing body.

5. Where Partners do not have a security classification scheme which includes handling rules the following points should be considered:
   
   - Ensure that unauthorised staff and other individuals are prevented from gaining access to personal data
   - Ensure visitors are received and supervised at all times in areas where personal data is stored
   - Ensure that all computer systems that contain personal data be password-protected. The level of security should depend on the type of data held, but ensure that only those who need to use the data have access.
   - Do not leave your workstation/PC signed on when you are not using it.
   - Lock away disks, tapes or printouts when not in use.
   - Ensure all new software is virus-checked prior to loading onto an Authority machine. Do the same for disks.
   - Exercise caution in what is sent via email and to whom it is sent, do not transmit personal data by email.
   - Check that the intended recipient of a fax containing personal data is aware that it is being sent and can ensure security on delivery.
   - Ensure your paper files are stored in secure locations and only accessed by those who need to use them.
- Do not disclose personal data to anyone other than the Data Subject unless you have the Data Subject’s consent, or it is a registered disclosure, required by law, or permitted by a Data Protection Act 1998 exemption.
- Do not leave information on public display in any form. Clear your desk at the end of each day and lock sensitive material away safely.
INFORMATION SHARING PROTOCOL REVIEW GROUP

Claire Everitt
Senior Information Management Officer
Information Management
Leicestershire County Council
County Hall
Glenfield
Leicestershire
LE3 8TG
Tel: 0116 305 7593
Fax: 0116 305 7271
Email: ceveritt@leics.gov.uk

Ed Smith
Head of Information Governance
Legal Services
Leicester City Council
Room B4-07
New Walk Centre
Welford Place
Leicester
LE1 6ZG
Tel: 0116 252 7605
Fax: 0116 252 7936
Email: ed.smith@leicester.gov.uk

Anne Chafer
Information Assurance Manager
Leicestershire Constabulary
Force HQ
St. Johns
Enderby
Leicester
LE19 2BX
Tel: 0116 248 2775
Fax: 0116 248 2125
Email: data.protection@leicestershire.pnn.police.uk

Lynne Wray
Business Programme Manager - Information Services
Leicestershire Partnership NHS Trust
Maracis Corridor
Daisy Peake Building
Gipsy Lane
Leicester LE5 0TD
Tel: 0116 295 8984
Fax: 0116 225 6583
Email: Lynne.Wray@leicspart.nhs.uk

Sara Jane Owens
Information Management Officer
Administration and Legal Services
Blaby District Council
Desford Road
Narborough
Leics
LE19 2EP
Tel: 0116 272 7709
Fax: 0116 272 7596
Email: sjo@blaby.gov.uk