APPENDIX ‘A8’

Data Sharing Protocol

This Protocol and Data Sharing Agreement Form (when completed & signed) comprise an agreement between organisations wishing to share data.

Data Sharing Protocol
Contents

Data Sharing Protocol

1. Document Control

Document

Client	East Herts Council
Project	Performance Management
Document	Data Sharing Protocol
Author	Trainee Performance Officer
Published Date	
Version	4

Change History

This document is to be submitted to the project team for approval and signoff. Thereafter amendments are to be approved by the appropriate Change Control procedures.

Issue	Date Of Issue	Comments / Reason For Change
1.0 –		Initial Draft
		Final Draft
2.0		Draft for Data Sharing Agreement Form
3.0	June 2009	Draft second year review

Distribution

Name	Position	Organisation
	Chief Executive	East Herts Council
	Directors	East Herts Council
	Heads of Service	East Herts Council

Abbreviations Used

Data Sharing Protocol

2. Background

1. What is a data sharing protocol

A data sharing protocol is ***an overall approach*** between organisations that are sharing data. It explains why data is being shared and sets out the principles and commitments organisations will adopt when they collect, store and disclose information.

Protocols also explain when information can be shared. Without such formal agreements, public organisations may find themselves falling short of common standards. Also, there may be confusion over responsibilities - both within and between organisations.

Protocols are intended to be a tool - not a bureaucratic hurdle to be overcome. The purpose of this strategy is to outline the Council's approach to data quality.

This Protocol requires the completion and signature of a Data Sharing Agreement Form (Appendix B)

2. Reasons for sharing information

Reasons for sharing information may include:

- Delivery of effective services
- Assuring and improving the quality of care and advice
- Monitoring and protecting public safety and well being
- Risk Management
- To avoid duplication of information gathering
- Managing and integrating the planning of services
- Contracting and commissioning the provision of services
- Auditing of accounts, care and performance
- Investigating complaints or actual/potential legal claims
- Teaching/staff development
- Statistical analysis
- Research

3. Purpose of East Herts Council's data sharing protocol

- To facilitate the sharing of data sets between agencies, groups and individuals
- To define the principles which underpin the exchange of information between parties who have signed up to the Protocol
- To set out the purpose for the exchange of personal information, the type of the information that may be exchanged and the purpose for which that information may be used.

- To establish procedures which will ensure that information is disclosed in line with statutory obligations and responsibilities
- To set out the responsibilities of organisations to implement internal arrangements to meet the requirements of the Protocol
- To make certain the roles and structures which will support the exchange of personal information between parties to the Protocol
- To specify the security procedures necessary to ensure that the confidentiality of personal information exchanged is maintained
- To state how this Protocol will be implemented, monitored and reviewed

4. Legislation

The Data Protection Act 1998 (DPA), in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data) in most formats e.g. paper, electronic, images (photographic/video) etc.

The key legislation governing the collection and use of personal information include:

- The Data Protection Act 1998
- The Human Rights Act 2000
- The Crime and Disorder Act 1998
- Common Law Duty of Confidentiality

The principle elements of the legislation are described in **Appendix A**.

5. Scope and application

There are three types of data sharing situations that are covered by this Protocol.

a) Non-personal data

Non-personal data is data that does not refer to living individuals. There are two types of non-personal data:

1. Data that has never referred to people; for example information on organisations, natural resources and projects.
2. Data about people that has been aggregated or tabulated in ways that make it impossible to identify the details of individuals.

Sharing of non-personal data for any purpose is covered by this Protocol.

b) De-personalised data

De-personalised data is data that describes individuals, but where identification of the individual is not possible by the organisations using the data, either from the data or in conjunction with other data or information they hold or are likely to acquire.

Note that although an organisation holding de-personalised data may not be able to identify individuals, there is a risk that a third party with other information may be able to. For this reason care may be needed with the storage and disposal of de-personalised information to comply with legal obligations.

Sharing of de-personalised data for any purpose is covered by this Protocol.

Both non-personal and de-personalised data are outside the scope of the DPA.

c) Personal data

Personal data is data about individuals who can be identified from the data, either directly or by pooling with other information available to the organisation. Personal information is defined as "data that relates to a living individual who can be identified from that data", for example personal data includes:

- Local identifier – system ID number
- Name
- Address
- Post code
- Date of Birth
- Other dates – such as date of death
- Sex
- Ethnic Origin
- Occupation

Personal data is specifically covered by the (DPA), which imposes a number of obligations and duties on those who hold such data and gives rights to individuals to know what data is held about them. The Act also has different provisions for sensitive personal data, for example:

- Racial or ethnic origin
- Political opinions
- Gender
- Religious or other similar beliefs
- Trade union membership
- Physical and mental health
- Sexuality
- Criminal offences and proceedings

In relation to this Protocol the DPA provides some exemptions for data used for the purpose of research (including statistical of historical purposes). These are given in section 33 of the Act and allow:

1. Personal data to be used for research, even if this was not obtained for this purpose.
2. Personal data used for research may be kept indefinitely.

Data Sharing Protocol
3. Purpose of Data Sharing Protocol

This Protocol ***applies to all Council Services.*** The Data Sharing Agreement Form will have blank fields for which specific information can be incorporated to/amended dependent on the specific needs to adapt the protocol for service use, while still following the main principles set out in the protocol structure.

Data Sharing Protocol
4. General Principles

Parties agreeing to this Protocol undertake to co-operate with each other and to fully and properly use its principles and procedures.

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

This Protocol provides an agreed framework for the process of agreeing, recording and actioning data sharing activities.

Complete freedom is given to the parties in deciding the specific circumstances of each data-sharing project that takes place between parties. Different data sharing projects may have different detail agreements, even where all parties are signatories to this Protocol.

Parties should only have access to personal information on a justifiable need to know basis, in order for them to perform their duties in connection with the services they are there to deliver.

All staff should be trained and be fully aware of their responsibilities to maintain the security and confidentiality of personal information.

Each party will operate lawfully in accordance with the 8 Data Protection Principles, see **Appendix A**.

Data Sharing Protocol
5. The Protocol

1. Lead person

Parties will nominate a lead person who will be responsible for the day-to-day management of the ***Data Sharing Agreement*** within their ***organisation***. The person

nominated will have sufficient seniority within the agency to influence policies and procedures at executive level.

2. Confidentiality

Personal information held by a party shall be deemed to have been provided in confidence, unless explicit or implied consent has been obtained. All parties accept this duty of confidentiality and will not disclose personal information without the consent of the person concerned, unless there are statutory grounds or other overriding justification for doing so. People requesting disclosure of personal information from parties signed up to the ***Data Sharing Agreement***, will respect this responsibility and will not seek to override the procedures which each party has in place to ensure that information is not disclosed illegally or inappropriately.

3. Consent

Unless statutory exemptions are applicable, all parties will endeavour to seek consent from the individual concerned to share their personal information. Consent will normally be obtained at the earliest opportunity and should be sufficient to cover the needs for a particular 'piece of work' or situation. It is essential that the need to repeatedly seek consent over minor issues should be avoided. In seeking consent to disclose personal information to another party signed up to **a *Data Sharing Agreement*** , an individual will be made fully aware of:

- the nature of the information that will be shared
- who the information will be shared with
- the purposes for which the information will be used
- other relevant details including their right to withhold or withdraw consent.

Based on this explanation, people have the right to withhold, comply or specify limitations as to the sharing and use of their information. Where there is evidence that a person does not have the capacity to give informed consent, (and recognising that no adult can give consent for another adult unless they have a power of attorney), it is good practice to involve relatives and other significant adults with senior professionals in the decision making process.

The outcome of the sharing of information in terms of forming an assessment or progressing a case needs to be recorded and fed back to the individual and those parties involved in the process.

4. Time limit on consent

Consent to disclose personal information will be limited to the duration of a 'piece of work' (specific involvement with any particular party until case closure).

- All parties agree that once the 'piece of work' for which consent was obtained has been completed that consent will be deemed to have lapsed.
- Upon the expiry of the deemed consent period or completion of the work which the information was required for, the information needs to be destroyed/deleted.

- In the event that a similar or subsequent additional work needs to be undertaken with that individual, a new consent to disclose must be obtained.

5. Recording of consent

The party obtaining explicit consent to disclose an individual's personal information will:

- Retain the original consent form on the individual's record
- Provide the person giving consent with a copy
- Provide a copy of the consent form to the other party/parties involved when the initial disclosure is made

All parties will ensure that the details (including any conditions) of any consent, or refused consent, are recorded on their systems in accordance with their policies and procedures.

6. Withdrawal of consent/add or amend restrictions

In the event that an individual:

- Withdraws his/her consent for their personal information to be shared or,
- Wishes to subsequently place/amend restriction upon the personal information to be shared

The party receiving such a request will immediately inform all other parties who are or may be affected and record the details on the individual's file.

In the case of consent being withdrawn, no further personal information should be disclosed unless there are statutory reasons for doing so, or legal exemptions can be applied.

In the case of a person applying restrictions on the use of their personal information, these restrictions should be complied with unless there are statutory reasons for doing so, or legal exemptions can be applied.

7. Disclosure of information without consent

Whilst all reasonable measures should be taken to gain consent, the DPA allows for the disclosure of personal information without the consent of individuals in certain circumstances. These are:

- Where there is concern about the risk of harm (including serious self- harm) to an individual, and information needs to be sought or shared in order to protect that individual or others in society
- For the detection and prevention of crime
- Where the court, under witness summons, has ordered that information should be disclosed

Disclosure without consent needs to be justifiable and the reasons recorded by professionals in each case on the individual's record. Sharing information without consent should be appropriate for the purpose and only to the extent necessary to achieve that purpose. These decisions should be audited and defended.

Decisions to disclose personal information without the consent of the individual concerned should be authorised by a senior member of staff (lead person) and/or the Legal Service section.

On disclosure of the information, the party providing the information will make the receiving party aware that disclosure is being made without consent and the reason(s) why.

Personal information will only be disclosed where the relevant agreed purpose for sharing clearly requires this. For all other purposes, information about individual cases will be anonymised.

8. Making disclosure

Parties will ensure that their staff, who are authorised to make disclosure of personal information will clearly state whether the information that is being supplied is fact, opinion, or a combination of the two.

9. Recording disclosure

Parties will ensure that all personal information that has been disclosed to them under an agreed protocol will be recorded accurately on the individual's manual or electronic record in accordance with their agencies policies and procedures, and contain:

- Details of the information
- Who gave the information
- Who received the information

10. Disclosure of a deceased's personal information

Parties must exercise caution when contemplating the disclosure of personal information relating to a deceased person. Although the DPA only applies to personal information of a living person, a duty of confidentiality may still apply after the person has died.

11. Complaints procedure

Parties will put in place efficient and effective procedures to address complaints relating to the disclosure or the use of personal information that has been provided under **a *Data Sharing Agreement***. In the event of a complaint relating to the disclosure or the use of an individual's personal information that has been supplied/obtained under **a *Data Sharing Agreement*,** all parties will co-operate and assist in order to resolve the complaint. All parties will ensure that service users will

be provided with information about the complaints procedures when consent is obtained or upon request.

12. Staff confidentiality agreement

All parties should ensure their staff (full/part time, Members, temporary, agency, students etc) who have access to, or are likely to come into contact with, personal information sign a confidentiality agreement as part of their terms and conditions of employment.

13. Staff awareness

Parties will ensure that all staff are aware of, and comply with, their responsibilities and obligations with regards to:

- The confidentiality of personal information about people who are in contact with their agency
- The commitment of the organisations/agency to only share information legally and within the terms of the protocol
- Information will be shared on a need-to-know basis
- Staff will be made aware that disclosure of personal information that cannot be justified, whether inadvertent or intentional will be subject to disciplinary action

14. Staff training

All parties will ensure that employees who need to share personal information are given appropriate training to enable them to share information legally, comply with any professional codes of practice and comply with any local policies and procedures.

15. Storage of Shared personal information

All personal information must be kept in a secure environment, where access is controlled and security measures are in place. Information for this Protocol covers any method of information creation or collection, including electronic capture and storage, manual paper records, video and audio recordings and any other images, however created. All parties will put in place policies and procedures governing the security, storage, retention and destruction of personal information.

16. *Access to Shared personal information*

All parties will put in place policies and procedures governing the access by their employees, and others, to personal information held within their manual and/or electronic systems and to ensure that access to such information is controlled and restricted to those who have a legitimate need to have access to the shared information and only for the original purpose it was intended for.

17. Accuracy of Shared Personal information

All stored personal data needs to have a recorded disposal date to ensure that personal information is up to date from any changes of circumstances or status to ensure quality of information. All parties will be responsible for putting in place policies and procedures to be followed when updating personal information and ensure any amendments will be made aware to all relevant parties to this agreement.

18. Transfer of personal information

All parties will put in place policies and procedures that govern the secure transfer of personal information both internally and externally. Such policies and procedures must cover:

- Internal and external postal arrangements
- Verbal, face-to-face, telephone
- Facsimiles
- Electronic mail (secure network or encryption)
- Electronic Work Transfer

19. Compromise of confidentiality

All parties will have in place appropriate measures to investigate and deal with inappropriate or unauthorised access to, or use of, personal information whether intentional or inadvertent.

In the event of personal information that has been shared under **a *Data Sharing Agreement*** having or may have been compromised, whether accidental or intentional, the party making the discovery will without delay:

- Inform the organisation who shared the information of the details
- Take steps to investigate the cause
- If appropriate, take disciplinary action against the person(s) responsible
- Take appropriate steps to avoid a repetition

On being notified that an individual's personal information has or may have been compromised, the original provider will assess the potential implications for the individual whose information has been compromised and if necessary:

- Notify the individual concerned
- Advise the individual of their rights
- Provide the individual with appropriate support

20. Use of personal information other than for an agreed purpose

Personal information shared under **a *Data Sharing Agreement*** will have been disclosed for a specific purpose and must only be used for that purpose. Personal information obtained under **a *Data Sharing Agreement*** will not be used by the receiving party as intelligence for the general use of that organisation. Parties

wishing to use information under this protocol for any purpose other than that defined, or to disclose that information to any person other than those authorised to receive that information must:

- Inform the originator of the information of their intention to use the information provided for a different purpose
- Obtain explicit consent from the individual(s) concerned before processing such information
- Only sufficient data needed for the project should be exchanged.
- Once data is used for its purpose it should be destroyed/deleted.

Parties who wish to use information provided to them under **a *Data Sharing Agreement***, for research or statistical purposes must ensure that policies and procedures are in place to guarantee that such personal information is anonymised.

21. Data Quality.

Data quality plays an important part towards contributing to the delivery of the Council's corporate priorities, with the key priority being to "Deliver customer focused services by maintaining and developing a well managed and publicly accountable organisation" and specifically the objective "Ensure effective performance management is used to deliver success and continuous service improvement year on year by 2%".

Data quality is the responsibility of all parties, whether they are inputting, extracting or analysing data from any of the Council's information systems. Each organization should be aware of their responsibility in relation to data quality, however some will play a greater role in data quality than others.

East Herts council has a data quality policy in place to act as a regulator for data. This means that data coming in and out of the authority has a set of standards for data to conform to. This will not only protect the interests of the public but also the interests of all partners who provide data to the council.

22. Data Sharing Guidance

Further detailed guidance on Sharing Personal Information can be found in the "Framework Code of Practice for Sharing Personal Information" issued by the Information Commissioners Office

23. Indemnity

Disclosure of personal information without consent must be justifiable on statutory grounds, or meet the criterion for claiming an exemption under the Data Protection Act. Without such justification, both the party and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

24. Review arrangements

This protocol will be reviewed annually. 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.

Data Sharing Protocol

Appendix A - Legislation

Legislation, under which most public sector agencies operate, defines the role, responsibility and power of the agency to enable it to carry out a particular function. The Data Protection Ac t 1998, in most cases, is the key to the use of personal information and links into most other legislation. The Act sets out to govern the collection, use, storage, destruction and protection of a living person's identifiable information (Personal Data) in most formats, e.g. paper, electronic, images (photographic/video) etc. Provided the necessary conditions of the Data Protection Act 1998 can be met, sharing of personal information is perfectly legal.

Data Protection Act 1998 (www.dataprotection.gov.uk)

The key principles of the Data Protection Act are:-

1.) Personal Data must be processed (e.g. collected, held, disclosed) fairly and lawfully and that processing must satisfy one of the conditions in Schedule 2 of the Act. The processing of sensitive data is further protected in that processing must also satisfy at least one of the conditions of Schedule 3 of the Act.

2) Personal Data shall be obtained and processed for only one or more specific and lawful purpose(s).

3) Personal Data shall be adequate, relevant and not excessive in relation to the specified purpose(s).

4) Personal Data shall be accurate and kept up to date.

5) Personal Data shall not be held for longer than is necessary.

6) Processing of Personal Data must be in accordance with the rights of the individual.

7) Appropriate technical and security measures should protect Personal Data.

8) Personal Data should not be transferred outside the European Union unless the recipient provides adequate protection.

Schedule 2 of the Data Protection Act 1998 specifies conditions Relevant to the Processing of Personal or Sensitive Data

a) The data subject has given his/her consent to the processing

b) The processing is necessary for:

- the performance of a contract to which the data subject is a party, or

- for the taking of steps at the request of the data subject with a view to entering into a contract.

c) The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract

d) The processing is necessary to protect the vital interests of the data subject.

e) The processing is necessary for the administration of justice for the exercise of any functions conferred on any person by or under any enactment for the exercise of any functions of the Crown, a Minister of the Crown or a government department for the exercise of any other functions of a public nature exercised in the public interest by any person

f) The processing is necessary for the purpose of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except when the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied. Schedule 3 of the Data Protection Act 1998 specifies additional conditions relevant for the processing of sensitive personal data, namely:-

a) The data subject has given his/her consent
b) Processing of sensitive personal data is necessary:-

- By right or obligation under law
- To protect specific vital interests of the individual or other persons, where consent cannot be given by or on behalf of the individual
- In the course of legitimate activities of specified non-profit organisations, with extra safeguards
- Information already publicly released by the individual
- Legal, judicial, government or crown reasons
- Medical purposes
- To monitor equality or opportunity
- By order of the Secretary of State.

Human Rights Act 2000 (www.humanrights.gov.uk)

Article 8.1 of the European Convention on Human Rights (given effect via the Human Rights Act 2000) provides that “everyone has the right to respect for his private and family life, his home and his correspondence”. This is however, a qualified right, i.e. there are specific grounds upon which it may be legitimate for authorities to infringe or limit those rights.

Article 8.2 of the European Convention on Human Rights provides “there shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder of crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

In the event of a claim arising from the Act that an organisation has acted in a way which is not compatible with the Convention rights, a key factor will be whether the organisation can show, in relation to its decisions(s) to have taken a particular course of action:-

a) That it has taken these rights into account;
b) That it considered whether any breach might result, directly or indirectly, from the action, or lack of action;
c) If there was the possibility of a breach, whether the particular rights which might be breached were absolute rights or qualified rights;
d) (if qualified rights) whether the organisation has proceeded in the way mentioned below

Crime and Disorder Act 1998 (www.homeoffice.gov.uk/cdact)

The Crime and Disorder Act 1998 introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in the local area.

Section 115 of the Act provides that any person has the power to lawfully disclose information to the police, local authorities, probation service or health authorities (or persons acting on their behalf) where they do not otherwise have the power, but only where it is necessary and expedient, for the purposes of the Act.

Whilst all agencies have the power to disclose, section 115 does not impose a requirement on them to exchange information, and responsibility for the disclosure remains with the agency that holds the information. It should be noted, however, that this does not exempt the provider from the requirements of the second Data Protection principle.

Common Law Duty of Confidentiality
All staff working in both the public and private sectors should be aware that they are subject to a Common Law Duty of Confidentiality, and must abide by this.

'In confidence'…Information is said to have been provided in confidence when it is reasonable to assume that the provider of that information believed that this would be the case, in particular where a professional relationship may exist e.g.doctor/patient, social worker/client, lawyer/client etc.

The duty of confidence only applies to person identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e. it is not possible for anyone to link the information to a specific individual. The duty of confidence requires that unless there is a statutory requirement or other legal reason to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute, but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g. to protect others from harm).

Whilst it is not entirely clear under law whether or not a common law duty of confidence extends to the deceased, the Department of Health and relevant professional bodies accept that there is an ethical duty to respect the confidentiality of the dead. Unless there is a sufficiently robust public interest justification for using identifiable information that has been provided in confidence then the consent of the individual concerned should be gained before disclosure of their information.

Schedules 2 and 3 of the Data Protection Act 1998 apply whether or not the information was provided in confidence. Where it is judged that an individual is unable to provide informed consent (due to age or condition), schedule 2 and 3 of the Data Protection Act 1998 must be satisfied (processing will normally need to be in the vital interest of the individual). 'Public functions' as outlined in schedule 2 and 'medical purposes' as outlined in schedule 3 of the Data Protection Act 1998 are also likely to be relevant.

Regulation of Investigatory Powers Act 2000 (www.homeoffice.gov.uk/ripa)

The Regulation of Investigatory Powers Act 2000 primarily deals with the acquisition and disclosure of information relating to the interception of communications, the carrying out of surveillance and the use of covert human intelligence. It is unlikely that this Act will have any implications on the sharing of personal information.