SPECIFIC INFORMATION EXCHANGE AGREEMENT

DATE:	SEPTEMBER 2012
FOR: (Name of Project and/or Group)	**ADULT SAFEGUARDING (INCLUDING SERIOUS CASE REVIEWS)**
BETWEEN:	Between Gloucestershire County Council (and agencies acting on their behalf); NHS Gloucestershire, Care Services, Gloucestershire Hospitals NHS Foundation Trust, 2gether NHS Foundation Trust, Gloucestershire Constabulary, the IMCA Service, Gloucestershire Fire, Gloucestershire Probation, Great Western Ambulance Service.

SITS BENEATH THE GLOUCESTERSHIRE INFORMATION SHARING PARTNERSHIP AGREEMENT

Indicate the Frequency of the Reviews:	Annually
Date of Next Review:	September 2013

This information exchange agreement reflects the reasons, processes and procedures for sharing personal data.

PURPOSE/REASON for SHARING State reasons for sharing including whether it is a statutory requirement to share or if it is voluntary stating the perceived benefits to the customer for the sharing.	The purpose of this protocol is to ensure that relevant information is shared so that professionals can work together to safeguard vulnerable adults from abuse. Any information that needs to be exchanged with agencies not directly party to this Agreement (i.e. agencies outside Gloucestershire) must still follow the guidance set out below.

DATA TYPE/ DESCRIPTION state exactly data to be shared. E.g. name, address etc.	The information to be exchanged or shared will include: clinical records, care plans or social care assessment documents which the person holding the record considers are relevant any information which enables them to ascertain the vulnerable adult's wishes and feelings, beliefs and values, or what these would be likely to be contact details of any relevant people, including family members if appropriate, and any relevant information they may be able to provide. The data will be shared both manually and electronically. Any electronic exchange of data will take place securely using the appropriate levels of encryption. All data will be stored securely.
DATABASE(S) USED	ERIC

CONSENT/LEGAL BASIS The legal basis for sharing personal data, State legislation that supports the sharing e.g. wellbeing power Local Government Act 2000. State the Schedule 2 (and Schedule 3 if sensitive personal data is to be shared) that allows the sharing e.g. See listing on page 25. How individuals will be informed of the sharing of data where required	Data Protection Act 1998 Human Rights Act 1998 No Secrets 2000 (government guidance) Common Law duty of confidence Mental Capacity Act 2005 Crime & Disorder Act 1988 The Police and Criminal Evidence Act 1984 In line with the Mental Capacity Act 2005, this protocol will only apply to individuals over the age of 16. Wherever possible informed consent to share information should be obtained from the vulnerable adult, however there may be situations where: • consent is withheld or • the person is unable to give informed consent Information may still be shared between professionals if consent is withheld **if** the team manager responsible for coordinating believes that: • there is a high risk of serious harm to the vulnerable person, or • consent was withheld under duress, or • other vulnerable adults or children are at risk. **OR** • when the courts have made an order, or • to prevent or detect or prosecute a serious crime. Absolute assurances of confidentiality cannot be given, especially where other vulnerable adults or children may be at risk. If consent is **withheld** and the risk of harm is assessed as low at that time, the team manager should consider what can be offered to the vulnerable adult to enable them to get help in the future. If the person is **unable to give informed consent** and is assessed as lacking capacity to consent, but information needs to be shared in order to prevent or protect them from abuse, then the 'best interest' principle must be followed.
SOFTWARE FORMAT USED **e.g. Word, Excel, CSV, etc.**	WORD
ENCRYPTED or UNENCRYPTED If unencrypted state why and how this will comply with GovConnect (if applicable)	ENCRYPTED

PHYSICAL TRANSFER METHOD **e.g. Memory Stick, Tape, Network, NHSNet, Laptop PC** State the process of exchange, taking account of threats and vulnerabilities in the proposed communication methods and ensuring adequate safeguards to protect the information during transit and storage are in place.	All exchanges will take place using Government Connect approved secure email systems within the Government Secure Intranet, e.g.GCSX, NHSnet, PNN, CJSM.
QUALITY include a statement to commit to the accuracy and completeness of the data exchanged, including a process for informing all relevant parties of any inaccuracies identified	All data exchanged must be accurate, valid, reliable, timely relevant and complete; the responsibility for ensuring this remains with the lead individual.
FREQUENCY OF DATA SHARING **e.g. monthly, weekly. Etc.**	As necessary
RETENTION state the person or authority who is responsible for keeping the master file and the period of retention of data – Any copies held by other members of the project or group must destroy their copies at the same time.	Retention and disposal of information will be in line with Gloucestershire County Council's Records Management Policy or the equivalent policy within partner agencies.
MONITORING Who will monitor that the processes above are taking place and are effective? What checks will be made?	This protocol will be reviewed in line with the Multi-Agency Safeguarding Adults Policy and Procedures, and within a maximum of 12 months of its approval. Compliance with this protocol will also be audited in line with the policy and procedures
SECURITY, INCIDENT MANAGEMENT & RESOLUTION PROCESS How will any breaches of security, inappropriate disclosure or loss of data be reported and managed? What will be the procedure to update this protocol in the light of any findings?	Any breaches in security, inappropriate disclosures or losses of data will be dealt with in line with either Gloucestershire County Council's Information Security Procedure or the equivalent partner agency's policy. (The GCC Information Security Procedure also includes, at Stage 5, a process for Post Incident Review and Learning, any finding from which would feed into a protocol review if appropriate)
AWARENESS TRAINING State how awareness of this data sharing agreement will be raised amongst staff	This protocol will: Form an appendix of the Multi Agency Safeguarding Adults Policy and Procedures Feed into specific Multi-Agency Safeguarding Adults training

DATA SUBJECT ACCESS REQUESTS State how the individual will access their information and include a statement which identifies the rights of the data subjects.	Any subject access requests will be dealt with in line with either the Gloucestershire County Council Access to Personal Information (Subject Access) Policy or the equivalent policy within partner agencies.
PRINCIPLE 8 OF THE DATA PROTECTION ACT 1998:	DATA SHOULD NOT BE TRANSFERRED TO OTHER COUNTRIES WITHOUT ADEQUATE PROTECTION

I the undersigned certify that the personal data being received will not be disclosed to unauthorised persons. The Data and their Purposes of Use are Notified under the Data Protection Act 1998 and my organisation/company is committed to compliance with the Data Protection Principles.	
DATE	
SIGNATURE	
JOB TITLE For and on behalf of: **ORGANISATION**	
DATE	
SIGNATURE	
JOB TITLE For and on behalf of: **ORGANISATION**	

GLOSSARY OF TERMS

Within this document, the following definitions apply:

Personal Data or personal information	Data which relates to a living individual who can be identified from that data or that data together with other information which is in possession, or is likely to come into the possession of the Data Controller
Sensitive Personal Data	Personal data consisting of : Racial or ethnic origin of data subject Political opinion Religious beliefs or other beliefs of a similar nature Membership of a trade union Physical or mental health or condition Sexual life Commission or alleged commission of any offence Any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court is such proceedings
Data Controller	Any person (including company organisation or individual) who (either alone or jointly or in common with other persons) determines how and for what the purposes any personal data is to be processed.
Data Processor	Any person (other than an employee of the Data Controller) who processes the data on behalf of the Data Controller.
Processing	Means obtaining, recording, holding the information or data or carrying out any operation on the information including organisation, adaptation or altering retrieval, consultation, use disclosure alignment combining, blocking or erasure or destruction of information or data.
Data Subject	An individual who is the subject of the personal data

The Principles of the Data Protection Act 1998

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

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

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

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

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

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Schedule 2 conditions for processing personal data:

- The individual who the personal data is about has consented to the processing.
- The processing is necessary:
  - in relation to a contract which the individual has entered into; or
  - because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to authority (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

Schedule 3 conditions for processing sensitive personal data

- The individual who the sensitive personal data is about has given **explicit** consent to the processing.
- The processing is necessary so that you can comply with employment law.
- The processing is necessary to protect the vital interests of:

  - the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
  - another person (in a case where the individual's consent has been unreasonably withheld).

- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition.
- The individual has deliberately made the information public.
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights.
- The processing is necessary for administering justice, or for exercising statutory or governmental functions.
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality.
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.