

## Schedule 3 - Specific Information Exchange Agreement

<b>Date:</b>	April 2012
<b>For:</b> (Name of Project and/or Group)	<b>Hard of Hearing Service</b>
<b>BETWEEN:</b>	Gloucestershire County Council (GCC) and Gloucestershire Deaf Association (GDA)

Sits beneath the Gloucestershire Information Sharing Partnership Agreement

<b>Indicate the Frequency of the Reviews:</b>	Annual
<b>Date of Next Review:</b>	March 2013

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

<p><b>PURPOSE/REASON for SHARING</b></p> <p>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.</p>	<p>Commissioned statutory service for hard of hearing environmental aids assessments. It is not a statutory requirement to share the information – CSOs ask all new referee's for permission to pass details on to GDA. If permission declined the customer is informed the referral will be sent to the locality but the wait will be longer.</p>
<p><b>DATA TYPE/ DESCRIPTION</b></p> <p>state exactly data to be shared. E.g. name, address etc.</p>	<p>Name, address, disabilities reason for referral and any relevant history.</p>
<p><b>DATABASE(S) USED</b></p>	<p>ERIC by GCC and Microsoft shared server by GDA – protected by firewalls; Norton Security software and virus checking and BT business hub firewall.</p>
<p><b>CONSENT/LEGAL BASIS</b></p> <p>The legal basis for sharing personal data, State legislation that supports the sharing e.g. wellbeing power Local Government Act 2000.</p> <p>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.</p> <p>How individuals will be informed of the sharing of data where required</p>	<p>Under the Data Protection Act 1998, Gloucestershire County Council remains the Data Controller for all data relating to the provision of adult social care.</p> <p><i>The data subject has given consent (or explicit consent if the personal data is sensitive) to the processing.</i></p> <p><i>The processing is necessary in order to protect the vital interests of the data subject or another person</i></p> <p>At point of contact/assessment</p>
<p><b>SOFTWARE FORMAT USED</b></p> <p>e.g. Word, Excel, CSV, etc.</p>	<p>WORD</p>

<p><b>ENCRYPTED or UNENCRYPTED</b> If unencrypted state why and how this will comply with GovConnect (if applicable)</p>	<p>Each file will be password protected when stored on GDA server. Files sent to GDA via Winzip will be encrypted using a minimum of 12 characters being a mixture of letters and numbers.</p>
<p><b>PHYSICAL TRANSFER METHOD</b> <b>e.g. Memory Stick, Tape, Network, NHSNet, Laptop PC</b> 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.</p>	<p>Winzip</p>
<p><b>QUALITY</b> 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</p>	<p>Regular meetings either weekly initially, to be reviewed after 3 months with a view to reducing to fortnightly.</p>
<p><b>FREQUENCY OF DATA SHARING</b> <b>e.g. monthly, weekly. Etc.</b></p>	<p>Data will be sent over weekly in an encrypted winzip file.</p>
<p><b>RETENTION</b> 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.</p>	<p>Retention and disposal of information will be in line with the Community &amp; Adult Care Directorate <a href="#">Records Management Policy</a> guidance or the equivalent policy within partner agencies.</p>
<p><b>MONITORING</b> Who will monitor that the processes above are taking place and are effective? What checks will be made?</p>	<p>Hard of Hearing Screening Manager in GCC and GDA worker</p>
<p><b>SECURITY</b> A process for managing breaches of security, inappropriate disclosure of data and loss of data</p>	<p>Any breaches in security will be dealt with in line with either the Gloucestershire County Council <a href="#">Data Protection Breach Policy</a> or the equivalent partner agency's policy.</p>
<p><b>INCIDENT MANAGEMENT &amp; RESOLUTION PROCESS</b> How will any breaches of this agreement or principles of the Data Protection Act 1998 be reported and managed? What will be the procedure to update this protocol in the light of any findings?</p>	<p>Any breaches in security will be dealt with in line with either the Gloucestershire County Council <a href="#">Data Protection Breach Policy</a> or the equivalent partner agency's policy.</p>
<p><b>AWARENESS TRAINING</b> State how awareness of this data sharing agreement will be raised amongst staff</p>	<p>Process map to be shared with all staff involved</p>
<p><b>DATA SUBJECT ACCESS REQUESTS</b> State how the individual will access their information and include a statement which identifies the rights of the data subjects.</p>	<p>Any subject access requests will be dealt with in line with either the Gloucestershire County Council <a href="#">Access to Personal Information (Subject Access) Policy</a> or the equivalent policy within partner agencies.</p>
<p><b><u>PRINCIPLE 8 OF THE DATA PROTECTION ACT 1998:</u></b></p>	<p>DATA SHOULD NOT BE TRANSFERRED TO OTHER COUNTRIES WITHOUT ADEQUATE PROTECTION</p>

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.

<b>DATE</b>	
<b>SIGNATURE</b>	
<b>JOB TITLE: Operations Manager</b> <b>Jenny Hopkins</b> For and on behalf of: <b>PROVIDER ORGANISATION</b>	
<b>DATE</b>	
<b>SIGNATURE</b>	
<b>JOB TITLE: Caldicott Guardian</b> <b>Fiona Jones</b> For and on behalf of: <b>PURCHASER ORGANISATION</b>	

### **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 in 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.