Review date:
April 2016

Gloucestershire Information Sharing Partnership Agreement (GISPA)

Version 2.0

Gloucestershire Authorities Information Management Forum

Gloucestershire Information Sharing Partnership Agreement (GISPA)

Version 2.0

Foreword

Sharing personal information is essential for delivering effective and efficient public services that meet the needs of people and safeguard the individual. Christopher Graham, the UK Information Commissioner, has written that a reluctance to share information in clearly appropriate circumstances "is one of the biggest challenges facing the public service today".

The Gloucestershire Authorities Information Management Forum, a cross-sector group of information management and governance experts, developed the first version of the overarching Gloucestershire Information Sharing Partnership Agreement (GISPA) in 2010. This was designed to encourage the safe, lawful and secure sharing of personal information between the police, health services, local authorities and their partners.

In the most recent review of the GISPA it was decided to draw very heavily on the Welsh Accord on the Sharing of Personal Information (WASPI). The WASPI has been developed with the support of the Welsh Government and covers organisations involved in the protection, safety, health, education and social welfare of the people across Wales (including statutory, private and third sector organisations). Full acknowledgement and thanks is therefore given to our WASPI colleagues.

Adoption of the GISPA as a basis for sharing and for developing Specific Information Sharing Agreements (SISA), where they are required, is essential for building the common approaches and improvement across services that are needed to ensure practice is safe, legal and secures public confidence. Gloucestershire's Specific Information Sharing Agreement (SISA) template has also been completely revised and incorporates in-built guidance to assist accurate completion.

Contents

1 Introduction & Purpose

1.1 Introduction

The purpose of the Gloucestershire Information Sharing Partnership Agreement (GISPA) is to enable service-providing organisations directly concerned with the safeguarding, welfare and protection of the wider public to share relevant, minimum and appropriate personal information between them in a lawful, safe and informed way.

The GISPA can be adopted by all public sector organisations. In particular it concerns those organisations that hold information about individuals and who may consider it appropriate or necessary to share that information with others.

Adoption of the GIPSA will help ensure compliance with statutory and legislative requirements for disclosing personal data including the Data Protection Act 1998, the Human Rights Act 1998 and with common law duty of confidentiality. It also enables compliance with the Information Commissioner's statutory Data Sharing Code of Practice.

Its implementation adds significant value to the delivery of effective and efficient public services that meet the needs of those receiving them.

The conditions, obligations and requirements set out in this agreement and supporting documentation will apply to all appropriate staff, agency workers, volunteers and others working on behalf of the partner organisations including agents and sub-contractors.

The GISPA will be reviewed annually by the Gloucestershire Authorities Information Management Forum.

1.2 The Agreement for Sharing Personal Information

The GISPA identifies the commitments required by each organisation to enable sharing of personal information. Sign up and ownership is at the highest level.

It is a statement of the principles and assurances which govern the activity of information sharing. It ensures that the rights of all those who are involved in the process are protected.

The GISPA will be supported within organisations by Specific Information Sharing Agreements (SISAs).

SISAs focus on the purposes underlying the sharing of specific sets of information between multiple organisations. They are intended for operational use and document the processes for sharing regular information, the specific purposes served, the people they impact upon, the relevant legislative powers, what data is to be shared, the consent processes involved, any required operational procedures and the process for review.

1.3 Information Excluded from the GISPA

Under the GISPA, there is no requirement to develop SISAs to cover the exchange of information where it is considered to be either of an ad-hoc nature or on an infrequent basis. However, organisations must still consider the relevant compliance issues in line with the ICO's Data Sharing Code of Practice.

In addition there are two further broad categories of information relating to personal information that organisations may share without the need for protocols or agreements. These are:

Aggregated (Statistical) Information
Aggregated and management information is used to plan and monitor progress of the organisation in its delivery of services. This is generally outside the scope of the Data Protection Act 1998 on the basis that a living individual could not be identified from such data.

Depersonalised and Anonymised Information
Information that has had all personal information removed so as to render it anonymous and therefore outside the scope of the Data Protection Act 1998.

Care must be taken with all aggregated, depersonalised and anonymised information to ensure that it is not possible to identify individuals e.g. in areas of low population density/low occurrence, as this would then still be classed as personal information.

2. Organisation Commitments

2.1 Introduction

This section outlines the principle commitments that each signatory organisation will make by adopting the GISPA. When fully implemented these should ensure that the organisation's treatment of personal information is compliant with current legislation and good practice.

2.2 Individual Users' Rights

Each organisation will comply with the rights of the individual in a fair and consistent manner and in accordance with any specific legislative requirements, regulations or guidance. Each organisation must ensure that they have appropriate policies and procedures in place to facilitate both the protection and the exercising of these and other rights.

Each organisation must be clear and open with individuals about how their information will be used. In general terms an individual should be told the identity of the organisation collecting and recording the data. The reasons or purpose for doing so (including any statistical or analytical purposes), and any extra information that an individual needs in the circumstances to ensure that their information is being processed fairly. This is known as a 'Fair Processing Notice or Privacy Notice' and complies with Principle 1 of the Data Protection Act 1998.

Each organisation must also inform individuals about their additional rights in respect of legislation and how these may be exercised. This will include the provision of appropriate support in order that individuals may best exercise those rights e.g. providing information in alternative formats or languages, providing support in the form of advocacy or assisting them to make a subject access requested under Section 7 of the Data Protection Act 1998.

Individuals generally have the right to object under Section 10 of the Data Protection Act 1998, to the use and disclosure of certain personal information and need to be made aware of this right by participating organisations. It should not be assumed that individuals are content for their personal information to be used for purposes other than those directly associated with their receipt of services from the organisation to which they provided their information.

All individuals have the right to expect that information disclosed by them or by other parties about them to an organisation will be protected, managed and processed with the appropriate degree of privacy and confidence. However, individual's rights to prevent disclosure of their personal information may be overridden in certain circumstances in accordance with legislation and common law.

2.3 Consent

All individuals must be informed as to the circumstances in which their consent will be required before their personal information may be shared. The details provided must include what personal information is recorded and why, what future use will be made of it and the length of time it is likely to be retained. The individual should also have explained to them the possible consequences of refusing or withdrawing consent and the exceptional circumstances in which a decision may be taken to share without consent.

Individuals will be informed that they are entitled to limit the disclosure of their information in accordance with their preferences, except where exceptional circumstances apply.

Individuals have the right to object to information they provide in confidence being disclosed to others in a form that identifies them, even where the latter are providing essential care or services.

Information may only be shared without consent in circumstances where it is justified and compatible with the requirements of current legislation, common law and any current guidance.

SISAs should provide the conditions which must be met before information can be shared and the circumstances in which information can be shared without consent.

Reasons that lead to a decision to proceed with a disclosure without consent must be fully documented. Wherever practical and possible participating organisations must inform the individual of the decision and the reasons for it and indicate the legal basis on which the disclosure is permitted or required.

If an individual lacks capacity and is unable to consent to a specific disclosure/sharing of information, any decision to share personal information about them without consent can only be made if it is in their best interests.

The person reaching a decision as to the best interest of the individual will take into account the following:

- The individual's previously expressed or recorded wishes;
- Views of any legal guardian or a person holding valid Lasting Power of Attorney;
- Views of a carer or other person close to the individual, including paid carers;

Safeguarding Children
Normally personal information about children will not be shared without the consent of the child themselves (if they are over the age of 12) or a person with parental responsibility. However, in situations where there is reasonable cause to suspect that a child or young person is suffering or is likely to suffer significant harm, children's social care must carry out a section 47 investigation.

All agencies have a responsibility to inform children's social care and to share information if they are concerned that a child or young person is in need or at risk of harm. It is good practice to seek consent from the family before doing this, however if this could increase the risk to the child or young person, information should be shared without consent as safeguarding the child is paramount.

2.4 Staff and Others with Access to Information

Each organisation must have in place internal operational policies and procedures that will facilitate the effective processing of personal information which is relevant to the needs of the organisation, its managers, staff and users.

Staff contracts must contain appropriate confidentiality clauses that detail possible consequences of unauthorised or inappropriate disclosure of personal information.

Staff should be made aware of the DPA offences outlined in Appendix A.

Each organisation must ensure that all relevant staff receive training, advice and ongoing support in order to be made aware, and understand the implications of:

- This GISPA and SISAs. This should include any associated procedural requirements arising from their implementation;
- The law which applies generally and in relation to the performance of the specific statutory powers and functions of the participating organisation concerned;
- Any Codes of Practice or other associated legislation, regulations and guidance.

Each organisation must have in place disciplinary procedures which could be invoked if a member of staff intentionally breached the confidentiality of a service user or intentionally shared information in a manner that is incompatible with the Data Protection Act.

Where a partner organisation relies on a third party to process personal information on their behalf, the organisation must have an appropriate contract in place.

2.5 Data Protection Act Notification

Under the Data Protection Act 1998 every organisation that processes personal information must have an appropriate entry (Notification) in the Register of Data Controllers managed by the Information Commissioner's Office, unless they are exempt. It is the responsibility of each organisation to ensure that its entry is kept accurate and up to date, failure to do so is a criminal offence.

2.6 Subject Access Requests

Organisations must fully comply with all valid Subject Access Requests made under Section 7 of the Data Protection Act.

If a request is received by an organisation which would also cover another organisation's information they should inform, and request the views of, the other organisation prior to release of the information. Each organisation should do this within the statutory timescales.

Each organisation must have in place policies and procedures that will facilitate the effective processing of Subject Access requests.

2.7 Freedom of Information

This GISPA should be disclosed under the Freedom of Information Act and should become part of your Publication Scheme.

Where partner organisations are not bound by this legislation consideration should still be given to referencing this information on their website.

2.8 Records Management

Inaccurate, incomplete or out of date information can have a detrimental effect on individuals. Therefore each organisation is responsible for the quality and accuracy of the personal information it holds.

If it is discovered that information held is inaccurate, partner organisations must ensure that their records/case management systems are corrected or updated accordingly. The organisation will take reasonable steps to advise any other party known to have received or to be holding that information about the change which it is necessary to make.

All participating organisations will have policies and procedures in place which will make clear their approach to retention, storage and disposal of records.

2.9 Information Security

Each organisation must have in place a level of security commensurate with the sensitivity and classification of the information to be stored and shared.

Each organisation must ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, information risk management, systems development, role based security access levels, secure receiving and transfer of data and system specific security policies.

Each organisation must consider the impact on individuals' privacy before developing any new IT system or changing the way they handle personal information. Please note that the Information Commissioner's Office have advice and guidance on Privacy Impact Assessments available on their website.

It is accepted that each organisation will vary in size and complexity and this will be reflected in their policies, processes, procedures, organisational structures and how they achieve effective information security.

2.10 Professional Ethics and Codes of Conduct

Partner organisations will recognise that individual professionals are accountable to their regulatory body for complying with their respective codes of conduct. Each organisation will take into account these requirements before reaching any decision to share information accordingly.

3. GIPSA and SISA Process

3.1. Adoption of the GISPA

All organisations wishing to use a Specific Information Sharing Agreement (SISA) for the sharing of information will need to be signed up to the GISPA. When signing up to the GISPA each organisation must identify a Designated Person who will have responsibility for implementing and monitoring the organisation's commitments. This will include supporting the adoption and dissemination of the GISPA within the organisation.

This Designated Person will usually be the person with overall responsibility for personal information within the organisation, such as the Senior Information Risk Officer (SIRO) or Caldicott Guardian.

The Designated Person may delegate day to day responsibility to individuals with operational responsibility for Information Governance and Data Protection.

Each GISPA Designated Person for the organisation agrees to support the adoption, dissemination, implementation, and review of this GISPA and its requirements in accordance with its own internal and any other jointly agreed and authorised information governance standard and/or operational policies and procedures.

The Designated Person must satisfy themselves that, in adopting the agreed standards and good practice, their organisation will work towards the principles and assurance set out in the GISPA.

The 'Declaration of Acceptance and Participation' should be completed and signed by the Designated Person, to confirm adoption of the GISPA. A copy of this declaration is at the end of the GISPA.

Once this has been completed a copy should be sent to the Information Management Service at Gloucestershire County Council email: dataprotection-gcsx@gloucestershire.gcsx.gov.uk

A record will be held of all signatories by the Information Management Service. The GISPA, the register of signatories and associated documents will be published on Gloucestershire County Council's website.

3.2. SISA Process

Once an organisation has signed up to the GISPA, Specific Information Sharing Agreements (SISAs) can be created.

SISAs should be completed by individuals with an operational knowledge of how the sharing will take place. All organisations included in the SISA should contribute to the creation of the document.

The signatory should be a senior member of staff such as a Caldicott Guardian, Director or equivalent.

The SISA should be completed and signed by both sharing organisations. A signed copy should be held by both organisations. A copy of the SISA template can be found at the end of the GISPA.

Individual organisations are responsible for their own SISAs. Gloucestershire County Council's Information Management Service is only responsible for publishing this document and the template SISA.

Each organisation is responsible for the audit, monitoring and publishing of its own SISAs.

3.3 Concerns and Complaints

Any concerns or complaints received relating to the processing/sharing of any personal information will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation. Any complaints relating to non-compliance may also be raised with other partner organisations if appropriate.

4. Glossary of terms

DPA	Data Protection Act
GAIMF	Gloucestershire Authorities Information Management Forum
GISPA	Gloucestershire Information Sharing Partnership Agreement
MOPI	Management of Police Information
SISA	Specific Information Sharing Agreement

5. Document History

Date	Version	Change type	Details
20.06.10	0.1	Amendment	Appendices amended
12.08.10	0.2	Amendment	SISA changed, NHS version adopted
16.09.10	0.3	Amendment	More content placed at appendices and forms removed for LA use.
28.10.10	0.4	Amendment	Formatting for final version
01.11.10	1.0	Version 1	Published on Gloucestershire Constabulary website
15.12.11	1.1	Revision	Minor amendments to bring into line with Information Commissioner's Data Sharing Code of Practice, signatories transferred to webpage, appendices separated to ease use of Appendix C.
12.12.12	1.2	Revision	Ownership updated, Welfare Reform Act added
12.04.13	1.3	Revision	Ownership transferred from Gloucestershire Constabulary to Gloucestershire Authorities Information Management Forum.
11.01.15	2.0	Version 2	Re-write to reflect good practice in the Welsh Accord on the Sharing of Personal Information (WASPI) as approved by the Information Commissioner's Office.

Appendix A

Data Protection Act offences

- Section 55 (1)(a) to knowingly or recklessly, without the consent of the Data Controller, obtain or disclose personal information;

- Section 55 (1 (b) to knowingly or recklessly, without the consent of the Data Controller, procure the disclosure to another person;

- Section 55 (4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).

- Section 55 (5) A person who offers to sell personal data is guilty of an offence if
- (a) he has obtained the data in contravention of subsection (1), or
- (b) he subsequently obtains the data in contravention of that subsection.

Appendix B

Specific Information Sharing agreement[1]

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

Gloucestershire Specific Information Sharing Agreement

Purpose

The organisations involved have signed up to the overarching principles set out in the Gloucestershire Information Sharing Partnership Agreement and these principles must be adhered to. Once information is shared with another organisation they become the data controller of the shared copy of the information and are responsible and accountable for the use and protection of it.

This agreement:

- sets out the legislative basis for the legitimate sharing of personal information in specific circumstances between two or more data controllers.
- will be supplemented by relevant procedures and standards (section 6 & 8).
- is to be completed by Information Asset Owners (or their delegate), project, process or service managers or an Information Governance Specialist.
- can only be signed by a Caldicott Guardian or Director (or equivalent).

This sharing agreement is not appropriate in circumstances where:

- one organisation engages another to undertake work on its behalf; in these cases information governance must be detailed within a contract; or
- one-off sharing is needed.

[1] This agreement sits below the Gloucestershire Information Sharing Partnership Agreement version 2.0

1. Parties to the agreement:

	Name and address of organisation
Party 1 This will be the lead party and the officer completing the agreement will become the agreement owner.	
Party 2	

(add more rows as required)

2. Why is this sharing required?

Detail the reasons for sharing and teams involved, such as 'helps provision of service', 'meets statutory obligation' etc.

3. What information is to be shared?

☐ Personal Information

☐ Sensitive Personal Information (see definitions)

Please select all that apply and then describe the information below, e.g. name, date of birth, address, health details etc.

Description of the information to be shared:

4. Frequency

How often will the sharing take place? ***Please delete as appropriate***

Daily / weekly / fortnightly / monthly / quarterly / annually / ad hoc / other

If ad hoc or other, please detail the circumstances when sharing will be appropriate:

5. Legislative basis

Please select all that apply and provide the name of the relevant piece(s) of legislation below.

☐ Information **MUST** be shared by law

☐ Information **MAY** be shared by law

☐ Information **MAY** be shared, but only with CONSENT

Details of the relevant legislation:

Data Protection Schedules ***(You must identify the specific condition(s) that are being met, not insert a full list of all of the conditions).***

Specific Schedule 2 Condition(s) satisfied:

Specific Schedule 3 Condition(s) satisfied:

(***Only complete the Schedule 3 Condition if you will be sharing sensitive personal data).***

6. How the Principles will be met

Each Party will need to detail how the requirements below will be achieved. Links should be provided to relevant procedures. (Links to the organisations intranets will only be accessible to those with access).

Requirement	Party 1 -	Party 2-
Principle 1 – Fair Use Each party will ensure that individuals are informed about the use of their personal data and this sharing.	**Delete as appropriate:** • Explicit written consent is received. • Individuals are given a leaflet at the time of collection. • Individuals are informed over the telephone at the time of collection. • Information is available online. Link to privacy notices on website:	**Delete as appropriate:** • Explicit written consent is received. • Individuals are given a leaflet at the time of collection. • Individuals are informed over the telephone at the time of collection. • Information is available online. Link to privacy notices on website:

	• Posters are displayed in public areas, details: • n/a – not the organisation collecting the data • Other:	• Posters are displayed in public areas, details: • n/a – not the organisation collecting the data • Other:
Principle 2 – Specific Purpose	The point of contact for this agreement will ensure that the information is only used for the purposes that individuals are informed about, or as required by law. They will ensure that the organisation's Data Protection Notification, Registration Number , covers this use of personal data. Information sharing decisions will be documented for audit, monitoring and investigation purposes.	The point of contact for this agreement will ensure that the information is only used for the purposes that individuals are informed about, or as required by law. They will ensure that the organisation's Data Protection Notification, Registration Number , covers this use of personal data. Information sharing decisions will be documented for audit, monitoring and investigation purposes.
Principle 3 – Adequacy	The point of contact for this agreement will review the data being shared every to ensure that sufficient, but not too much, information is being shared.	The point of contact for this agreement will review the data being shared every to ensure that sufficient, but not too much, information is being shared.
Principle 4 – Accuracy Each organisation must ensure the accuracy of the information they hold.	Please describe how you ensure data is accurate e.g. Data Quality Strategy, regular data cleansing exercises, controls are in place for data entry, etc. Links: If the party notices any errors in the data they will notify the relevant point of contact within days of becoming aware.	Please describe how you ensure data is accurate e.g. Data quality strategy, regular data cleansing exercises, controls are in place for data entry, etc. Links: If the party notices any errors in the data they will notify the relevant point of contact within days of becoming aware.
Principle 5 – Retention Information will be kept in accordance with each party's retention schedule.	The point of contact for this agreement will ensure that suitable entries are within their organisation's retention schedule and these are adhered to. Link to retention schedule:	The point of contact for this agreement will ensure that suitable entries are within their organisation's retention schedule and these are adhered to. Link to retention schedule:
Principle 6 – Rights of the Individual	**Subject Access** The point of contact for this agreement will ensure that procedures are in place to manage Subject Access Requests. Link to procedures/form: If information supplied by another party	**Subject Access** The point of contact for this agreement will ensure that procedures are in place to manage Subject Access Requests Link to procedures/form: If information supplied by another party

	is captured by a request for information, reasonable endeavours should be made to consult with that party regarding the release. **S10 - Cease Processing** If a S10 request is received, the point of contact for this agreement will assess whether it is appropriate to inform the other parties to this agreement. **Automated Decision Making** The point of contact for this agreement will ensure that the reasons for any automated decision-making are made clear to individuals and they are informed of their right of appeal. **Complaints** Concerns from individuals about the accuracy of their personal information need to be referred to the originating organisation. They will in turn investigate and inform any recipients of the information, if it is concluded to be incorrect, so it can be corrected.	is captured by a request for information, reasonable endeavours should be made to consult with that party regarding the release. **S10 - Cease Processing** If a S10 request is received, the point of contact for this agreement will assess whether it is appropriate to inform the other parties to this agreement. **Automated Decision Making** The point of contact for this agreement will ensure that the reasons for any automated decision-making are made clear to individuals and they are informed of their right of appeal. **Complaints** Concerns from individuals about the accuracy of their personal information need to be referred to the originating organisation. They will in turn investigate and inform any recipients of the information, if it is concluded to be incorrect, so it can be corrected.
Principle 7 – Security Personal data must be kept secure at all times; collection; storage; use, sharing, transfer and disposal.	**The data will be shared by:** *(delete/add as appropriate)* • Secure file transfer • Secure email e.g. GCSx, Egress • Post • Encrypted removable media, e.g. memory stick • Secure access to system, name of system • As part of joint working arrangements, **Delete/add as appropriate:** The party meets the following information governance assurance standards : • N3 • PSN • ISO27001 Specific procedures for the security of personal data are detailed at . Approved transfer methods: (link)	**The data will be shared by:** *(delete/add as appropriate)* • Secure file transfer • Secure email e.g. GCSx, Egress • Post • Encrypted removable media, e.g. memory stick • Secure access to system, name of system As part of joint working arrangements, **Delete/add as appropriate:** The party meets the following information governance assurance standards : • N3 • PSN • ISO27001 Specific procedures for the security of personal data are detailed at . Approved transfer methods:

	Approved disposal methods: (link) **Add more links to specific guidance as required.** The point of contact for this agreement will ensure that suitable information security incident procedures are in place. Link:	(link) Approved disposal methods: (link) **Add more links to specific guidance as required.** The point of contact for this agreement will ensure that suitable information security incident procedures are in place. Link:
Principle 8 – Not to be transferred out of EEA	Data shall not be transferred to countries other than those in the European Economic Area and those countries in Europe identified in the European Commission's list of countries or territories providing adequate protection for the rights and freedoms of individuals in connection with the processing of personal data.	Data shall not be transferred to countries other than those in the European Economic Area and those countries in Europe identified in the European Commission's list of countries or territories providing adequate protection for the rights and freedoms of individuals in connection with the processing of personal data.

(Add more columns for each party as required. You may also need to change the orientation of the document to landscape)

7. Review

This sharing agreement will be reviewed every 3 years or earlier if a significant change occurs.

If the Constabulary are party to this agreement to satisfy MOPI requirements it will be reviewed annually.

8. Supplementary documents

This agreement is to be supplemented by appropriate supporting documents, which may include:

- Information Transfer Procedure, including detailed security arrangements
- Information Risk Assessment
- Privacy Impact Assessment
- Retention Schedule
- Information Flow Map

9. Document information

Document owner:	Named point of contact for Party 1, detailed in section 10.
Next review date:	

Version:	
Summary of changes:	

10. Point of contact for each party

	Name	Role	Contact Details
Party 1 - ***This will be the person who completed the agreement. (This person will be the document owner. They will be responsible for adherence to, review, monitoring and advice in relation to the agreement.)***			
Party 2 -			

11. Signatories

	Name	Role ***(Please delete as appropriate)***	Signature	Date
Party 1 -		**Caldicott Guardian / Director /or equivalent**		

Party 2 -		**Caldicott Guardian / Director /or equivalent**		

(add more rows as required)

Appendix 1 – Definitions of personal and sensitive personal data

Personal data

Any information that identifies a living individual. This includes, but is not limited to, name, data of birth, NI number, medical diagnosis, address, employee number.

You may think information has been anonymised, but the legal definition takes into account other data held by the organisation. Therefore, if you hold the key to identify people from the anonymised data, then it is still covered by the Data Protection Act.

Sensitive Personal Data

- racial or ethnic origin
- sexual life
- religious beliefs (or similar)
- physical or mental health/condition
- membership of a Trade Union
- political opinions or beliefs
- details of/proceedings in connection with an offence or alleged offence

Appendix 2 – Schedule 2 Conditions

- 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 the 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 necessary for the purposes of legitimate interests pursued by the organisation or party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Appendix 3 – Schedule 3 conditions

If you are processing sensitive personal data you must be able to meet one of the conditions in schedule 2 and one in schedule 3.

- 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.

Appendix C

Gloucestershire Information Sharing Partnership Agreement – Declaration of Acceptance and Participation form

Please return a signed copy of this form to the Information Management Service at Gloucestershire County Council email address: dataprotection-gcsx@gloucestershire.gcsx.gov.uk

Version 2.0:
This signature is hereby given as confirmation that [INSERT ORGANISATION NAME] is a signatory to the GISPA. I will be the signatory and representative for this organisation.
Signature:
Name:
On behalf of:
Date: