Gloucestershire Information Sharing Partnership Agreement (GISPA)

Version 4.1

Gloucestershire Information Governance Group

Gloucestershire Information Sharing Partnership Agreement (GISPA)

Version 4.1

Executive Summary

Sharing personal information is essential for delivering effective and efficient public services that meet the needs of people and safeguard the individual. Legislation for Health and Social Care, and Caldicott principles reinforce the need to share information for direct care, as it is well recognised that personal information is essential for the provision of safe and high quality health and care services.

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.

The GISPA draws very heavily on the Wales 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.

This version 4.1 has amendments to the SISA template to ensure accuracy in reflecting the GDPR and DPA 2018 principles and rights.

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 and their partners. 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 GISPA will help ensure compliance with statutory and legislative requirements for disclosing personal data including the General Data Protection Regulation (GDPR), the Data Protection Act 2018, the Human Rights Act 1998 and with the 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 Information Governance Group.

Each Partner confirms that its Data Protection Officer, Caldicott Guardian, SIRO or other equivalent role has reviewed and agrees with the provisions of this agreement.

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.

All Parties are considered a Data Controller in their own right under current Data Protection legislation.

All parties shall comply at all times with all applicable laws and regulations relating to processing of personal information and privacy in effect in England and Wales, including where applicable the guidance and codes of practice issued by the Information Commissioner, the Department of Health and other relevant bodies and shall not perform its obligations under this Agreement in such a way as to cause any other party to this Agreement to breach any of its obligations under such applicable laws, regulations or guidance.

The legal justification for sharing personal or special category data under this Agreement is specified as follows:

By signing and agreeing to the terms of the Agreement, All Parties hereby undertake that any specified data and information shall be treated with appropriate confidentiality, integrity and security, namely:

All Parties will use the same degree of care as it uses to protect its own strictly confidential information which is processed under current Data Protection legislation, to maintain the data in strict confidence.

All Parties shall not make any use of, or otherwise process, the data and information received other than for the agreed purpose.

All Parties shall restrict access to the data and information received solely to its staff members and/or the staff members of any authorised third party organisation who need to have such access in order to carry out the agreed purpose.

All parties are responsible for ensuring the accuracy, completeness and validity of the data.

By signing this Agreement, all parties will use its reasonable endeavours to ensure that appropriate security and confidentiality procedures are in place to protect the transfer and use of the personal data by the following:

Complying with the Data Security and Protection Toolkit (DSPT) as appropriate to its organisation type and adhering to robust information governance management and accountability arrangements, including effective security event reporting and management; and

Complying with the DSPT assessment, reporting and audit requirements relevant to its organisation type. Third parties shall internally audit their compliance annually and report on such audits to the provider.

LIABILITY

Each Party shall accept responsibility for its own acts and omissions.

Nothing in this agreement shall limit liability for death or personal injury resulting from negligence or for fraud.

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 Data Protection legislation 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 Data Protection legislation.

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.

In addition, extra consideration should be given to other datasets that maybe held by either organisation. The GDPR definition of personal data also includes individuals "who can be indirectly identified from that information in combination with other 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 Rights of the Individual

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 should include easily accessible details of all an individual's rights where they apply:

The right to be informed
Each organisation must be clear and open with individuals about how their information will be used. This should be in the form of a 'Privacy Notice' which complies with Articles 12 & 13 of the GDPR.

In general terms an individual should be told the following:

- The identity and contact details of the organisation collecting and recording the data
- The lawful basis for processing
- The contact details of the Data Protection Officer, where applicable
- Why their information is being collected and used, and for what purpose (including any statistical or analytical purposes)
- The type/categories of information being collected
- How long their information will be kept for

Who their information will be shared with**The right of access**The right to request a copy of the information held about them and how to request this.

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

Should a response not be received from a partner organisation – i.e. any relevant information that is accessible to but not used by the recipient partner will not be disclosed; instead the requestor will be notified that further relevant information may be requested from the partner organisation (who can ensure appropriate disclosure of the information).

The right to recification

The right to request the correction of inaccurate or incomplete information

The right to erasure

The right to be forgotten when there is no compelling reason for information to be retained

The right to restrict

Processing for a period of time if the individual is contesting its accuracy or lawfulness

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services

The right to object

To the use of their information when they feel it falls outside the organisation's remit or it has been used for direct marketing

Rights in relation to automated decision making (ADM) and profiling

You must identify whether any of your processing falls ADM or profiling and, if so, make sure that you:

give individuals information about the processing;

introduce simple ways for them to request human intervention or challenge a decision;

carry out regular checks to make sure that your systems are working as intended.

Each organisation must also inform and 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 request.

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.

Each organisation will appoint a Data Protection Officer, if appropriate, and publish contact details.

2.3 Consent

Where consent is sought under Data Protection legislation, each organisation shall comply with the requirements for valid consent including:

- The GDPR sets a high standard for consent and often it will not be the appropriate lawful basis. Ensure there is no other lawful basis before using consent.
- Offering individuals a real choice and control.
- Don't use pre-ticked boxes or any other method of default consent.
- Explicit consent requires a very clear and specific statement of consent.
- Keep your consent requests separate from other terms and conditions.

- Be specific and 'granular' so that you get separate consent for separate things. Vague or blanket consent is not enough.
- Be clear and concise.
- Name any third party controllers who will rely on the consent.
- Make it easy for people to withdraw consent and tell them how.
- Keep evidence of consent – who, when, how, and what you told people.
- Keep consent under review, and refresh it if anything changes.
- Avoid making consent to processing a precondition of a service.
- Public authorities and employers will need to take extra care to show that consent is freely given, taking into account the balance of power between the individual and the organisation.

. The SISA shall detail lawful basis for processing, and condition(s) satisfied for processing special categories of data.

2.4 Safeguarding & Best interests

In terms of statute, Data Protection legislation sets out circumstances in which the use of data may be lawful. Additionally, the common law generally requires consent for disclosure, which may be explicit or implied. Each organisation must be sure that any use of data falls into the relevant Data Protection legislation categories and meets the common law requirement for consent except where disclosures are required by law or in the public interest.

Best interests

If an individual lacks capacity and is unable to consent to a specific disclosure/sharing of information, where consent is the lawful basis, any decision to share personal information about them 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.

The Children Act (2004) provides the legal basis for how social services and other agencies deal with issues relating to children.

Reasons that lead to a decision to proceed with a disclosure 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.

2.5 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 receives 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 current Data Protection legislation.

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.

2.6 Data Protection Fee

The Data Protection (Charges and Information) Regulations 2018 places a legal requirement on data controllers to pay the Information Commissioner's Office an annual data protection fee.

A 3 tier payment system exists based on the size of an organisation, its annual turnover and the volume of data processed.

2.7 Data Privacy Impact Assessments (DPIA)The GDPR, section 35, introduces a new obligation to do a DPIA before carrying out types of processing likely to result in high risk to individuals' rights and freedoms. This is a key part of the new focus on accountability and data protection by design.

A DPIA is a way to systematically and comprehensively analyse your processing and help you identify and minimise data protection risks.

DPIAs should consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

A DPIA must:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping you demonstrate accountability.

2.8 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.

2.9 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.

2.10 Information Security & Breaches

Each organisation must have in place a level of security that is compliant with Article 6(1)(f) integrity and confidentiality. 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 see section 2.7.

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the Information Commissioners Office. Each organisation must ensure that this can done within 72 hours

of becoming aware of the breach and inform any partner organisation if their information has been affected by the breach.

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.

2.11 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. GISPA 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 Data Protection Officer, Senior Information Risk Officer (SIRO) or Caldicott Guardian or equivalent.

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: DPO@gloucestershire.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

Organisations will promptly share any information governance risks or incidents of significance identified to any partner that is accountable for that risk(s)/incident(s).

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

GDPR	The General Data Protection Regulation
DPA	The Data Protection Act 2018
GAIMF	Gloucestershire Authorities Information Management Forum
GISPA	Gloucestershire Information Sharing Partnership Agreement
DSPT	Data Security and Protection Toolkit
MOPI	Management of Police Information
SISA	Specific Information Sharing Agreement

Access [to information] – refers to information being made available, which could be through authorisation (such as being given a key or credentials to access an information asset) or through insufficient information security measures.

Processing [of information] is defined as:

> *'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

Sharing [of information] – the act of giving information to another party.

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.
30.09.16	3.0	Version 3	Revision of version 2.0 by the Gloucestershire Information Governance Group
16.05.18	3.1	Amendment	Draft to reflect GDPR
10.07.2018	3.2	Amendment	Amended by Gloucestershire Information Governance Group to reflect GDPR and Data Protection Act 2018
23.07.2018	4.0	Version 4	Updated to reflect GDPR and Data Protection Act
15/01/2020	4.1	Amendment	Amendments to the accurately reflect the GDPR rights.

This document is available on line http://www.gloucestershire.gov.uk/informationsharing in line with NHS accessibility standards.

Appendix A

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 specific information sharing 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
- 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 specific information 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.

LIABILITY

Each Party shall accept responsibility for its own acts and omissions.

Nothing in this agreement shall limit liability for death or personal injury resulting from negligence or for fraud.

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.* *Each party is responsible for ensuring the sharing is documented for their own record of processing.* *Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers and document within this agreement their respective responsibilities for compliance.*	
Party 2	
Party 3	

(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 Data

☐ Special Categories of Personal Data (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. Lawful basis

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

For information on the most appropriate lawful basis, see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

Article 6

☐ Information is being processed to fulfil a legal obligation

☐ Information is being processed to carry out a public task

☐ Information is being processed to carry out a contract

☐ Information is being processed with the consent of the individual

☐ Information is being processed to protect an individual's vital interests

☐ Information is being processed for legitimate interests

If using legal obligation for you lawful basis, please provide details of the relevant legislation:

Article 9

☐ the data subject has given explicit consent to the processing

☐ processing is necessary for the purposes of employment and social security and social protection law

☐ processing is necessary to protect the vital interests of the data subject or of another natural person

☐ processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body

☐ processing relates to personal data which are manifestly made public by the data subject;

☐ processing is necessary for the establishment, exercise or defence of legal claims

☐ processing is necessary for reasons of substantial public interest

☐ processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services

☐ processing is necessary for reasons of public interest in the area of public health

☐ processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Will this sharing be using criminal conviction data?

Yes / No

If yes, your Information Governance Adviser will liaise with you to gather more information.

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-	Party 3-
Principle a – Lawful, Fair and Transparent Processing 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 give a privacy notice 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:	**Delete as appropriate:** • Explicit written consent is received. • Individuals are given a privacy notice 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:	**Delete as appropriate:** • Explicit written consent is received. • Individuals are given a privacy notice 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:
Principle b – Purpose limitation	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 has paid a Data Protection Fee and given contact details of the Data Protection Officer (if required) to the Information Commissioner. Registration Number , They will ensure that the organisation's Data Protection Notification covers this	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 has paid a Data Protection Fee and given contact details of the Data Protection Officer (if required) to the Information Commissioner. Registration Number , They will ensure that the organisation's Data Protection Notification covers this use of personal data.	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 has paid a Data Protection Fee and given contact details of the Data Protection Officer (if required) to the Information Commissioner. Registration Number , They will ensure that the organisation's Data Protection Notification covers this use

	use of personal data. Information sharing decisions will be documented for audit, monitoring and investigation purposes.	 Information sharing decisions will be documented for audit, monitoring and investigation purposes.	of personal data. Information sharing decisions will be documented for audit, monitoring and investigation purposes.
Principle c – Data Minimisation	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.	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 d – 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.	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 e – Storage limitation 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. <u>Link to retention schedule:</u>	The point of contact for this agreement will ensure that suitable entries are within their organisation's retention schedule and these are adhered to. <u>Link to retention schedule:</u>	The point of contact for this agreement will ensure that suitable entries are within their organisation's retention schedule and these are adhered to. <u>Link to retention schedule:</u>
Principle f – Integrity and Confidentiality 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, Egress, Government White List • Post • Encrypted removable media, e.g. memory stick • Secure access to system, name of system	**The data will be shared by:** *(delete/add as appropriate)* • Secure file transfer • Secure email e.g. Egress, Government White List • Post • Encrypted removable media, e.g. memory stick • Secure access to system, name of system	**The data will be shared by:** *(delete/add as appropriate)* • Secure file transfer • Secure email e.g. Egress, Government White List • 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 • Cyber Essentials Specific procedures for the security of personal data are detailed at . Approved transfer methods: (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:	• As part of joint working arrangements, **Delete/add as appropriate:** The party meets the following information governance assurance standards : • N3 • PSN • ISO27001 • Cyber Essentials Specific procedures for the security of personal data are detailed at . Approved transfer methods: (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:	• As part of joint working arrangements, **Delete/add as appropriate:** The party meets the following information governance assurance standards : • N3 • PSN • ISO27001 • Cyber Essentials Specific procedures for the security of personal data are detailed at . Approved transfer methods: (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:
Individuals Rights	You have a process in place so staff can understand and process individual's rights. You need to be transparent about these, which need to be in your privacy notice. More information in section 8.	You have a process in place so staff can understand and process individual's rights. You need to be transparent about these, which need to be in your privacy notice. More information in section 8.	You have a process in place so staff can understand and process individual's rights. You need to be transparent about these, which need to be in your privacy notice. More information in section 8.

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

7. International Transfers

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

Transfers outside of the EU may be made where:

- the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

- the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

Data shall not be transferred to countries other than those in the European Union 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.

8. Rights

The right to be informed
The point of contact for this agreement will ensure that a privacy policy is in place so that individuals are informed about the use of their personal data.

The right of access
The point of contact for this agreement will ensure that procedures are in place to manage Subject Access Requests.

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.

The right to rectification, erasure and restriction
Requests from individuals about, the accuracy, erasure and restriction of their personal information will be referred to the originating organisation. They will in turn consider the request and information any recipients of the outcome.

The right to data portability
The point of contact for this agreement will ensure that procedures are in place to manage requests for portability of data.

The right to object
If an objection to processing is received, the point of contact for this agreement will assess whether it is appropriate to inform the other parties to this agreement.

Rights in relation to automated decision making and profiling
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.

9. 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.

10. 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
- Data Protection Privacy Impact Assessment
- Retention Schedule
- Information Flow Map

11. Document information

Document owner:	Named point of contact for Party 1, detailed in section 12.
Next review date:	
Version:	
Summary of changes:	

12. 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 -			
Party 3 -			

13. Signatories

	Name	Role *(Please delete as appropriate)*	Signature	Date
Party 1 -		Caldicott Guardian / Director of		
Party 2 -		Caldicott Guardian / Director of		
Party 3 -		Caldicott Guardian / Director of		

(add more rows as required)

Appendix B – Definitions & Offences

Personal data

Is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

Special Categories of Personal Data

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (when used for ID purposes)
- health
- sex life
- sexual orientation

Offences under the DPA 2018

Section 119: Obstructing the Commissioner in inspecting personal data to discharge an international obligation

The Commissioner may inspect personal data where the inspection is necessary in order to discharge an international obligation of the United Kingdom, subject to the restriction in subsection (2). Section 119 (6) states that it is an offence (a)intentionally to obstruct a person exercising the power under subsection (1), or (b)to fail without reasonable excuse to give a person exercising that power any assistance the person may reasonably require.

Section 132: Prohibition placed upon the Commissioner, or the Commissioner's staff against disclosing information obtained in the course of their role (which is not available to the public

By former or current ICO staff who disclose data obtained during the course of their duties, it is an offence for a person knowingly or recklessly to disclose information.

Section 144: False statement made in response to an information notice

It is an offence for a person, in response to information notice from the Commissioner, to make or recklessly make, a statement which they know to be false in a material respect.

Section 148: Destroying or falsifying information and documents etc

Under Section 148 (2) (a) it is an offence for a person to destroy or otherwise dispose of, conceal, block or (where relevant) falsify all or part of the information, document, equipment or material. Section 148 (2) (b) makes to cause or permit the actions set pout in the previous subsection.

Section 170: Unlawful obtaining etc of personal data

It is an offence to knowingly or recklessly obtaining, disclosing or procuring personal data without the consent of the data controller, and the sale or offering for sale of that data.

Section 171: Re-identification of de-identified personal data

Section (5) states that it is an offence for a person knowingly or recklessly to process personal data that is information that has been re-identified.

Section 173: Alteration etc of personal data to prevent disclosure to data subject

Section 173 (3) makes it a criminal offence for organisations (persons listed in Section 173 (4)) to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure.

Section 184: Prohibition of requirement to produce relevant records

Section 184 (1) makes it an offence for a person to require another to provide them with or give them access to a relevant record linked to the employment, continued employment of one of their employees or a contract for the provisions of services to them. Section 184 (2) makes it an offence for a person to require another to provide them with or access to a relevant record if the requestor is involved in the provision of goods, facilities or services to the public or the requirement is a condition of providing or offering to provide goods, facilities or services to the other person or a third party.

Schedule 15, Paragraph 15. Powers of Entry and Inspection

It is an offence under paragraph 15 (1) for a person to intentionally obstruct a person in the execution of a warrant issued under this Schedule or to fail without reasonable excuse to give a person executing the warrant such assistance as may be required. Under paragraph 15 (2) it is an offence for a person to make a statement in response to a requirement under paragraph 5(2(c) or (d) or 3(c) or (d) which the person knows to be false in a material respect or recklessly make such a statement.

There are no custodial sentences in respect of offences under DPA 2018 and no powers of arrest; all offences are punishable only by a fine

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: DPO@gloucestershire.gov.uk

Version 4.1:
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:
Organisation:
Date: