Cambridgeshire Information Sharing Framework

CONTENTS

1. WELCOME

Public sector organisations in Cambridgeshire have worked together to develop this Information Sharing Framework to create a positive culture of sharing information and facilitate more effective data sharing practice across the county with the aim of improving service delivery.

The Framework applies to all information being shared by partner organisations and it will establish the types of data we will share, how we handle data and the legislation which allows us to do so.

The partner organisations involved in developing the Framework are:

- Cambridge City Council
- Cambridgeshire Constabulary
- Cambridgeshire County Council
- Cambridgeshire Fire and Rescue Service
- East Cambridgeshire District Council
- Fenland District Council
- Hinchingbrooke Health Care NHS Trust
- Huntingdonshire District Council
- NHS Cambridgeshire and NHS Peterborough
- South Cambridgeshire District Council

2. INTRODUCTION

This Information Sharing Framework has been developed to ensure that information is being shared appropriately and in line with best practice. The document aims to establish consistent principles and practices to govern any sharing of personal and non-personal information taking place within and between partner organisations across Cambridgeshire. The ethos of the Framework is for partners to share information in all situations to improve service delivery and resident outcomes and to support safeguarding in Cambridgeshire, except where it would be illegal to do so. **Remember, refusing to share any data can be a risk just as much as the opposite action of sharing too much data.**

This Information Sharing Framework is considered to be the overarching framework for the organisations which sign up to it. Any existing data sharing agreements should ensure that they comply with these principles as and when they are reviewed.

This Framework applies to information shared by partner organisations excluding any information which is already in the public domain. Sharing is not restricted solely to information classified as personal data by the Data Protection Act. This includes the following information:

a) All information processed by the organisations, including electronically (e.g. computer systems, CCTV, audio etc) or in manual records;

b) Anonymised, including aggregated data. The considerations, though less stringent, must take into account factors such as commercial or business sensitive data, and the effect of many data sets being applied.

Sharing information between organisations can improve outcomes in service delivery; however, sharing must be undertaken lawfully, respecting the rights of individuals and protecting the security of their information.

It is worth bearing in mind that the legislation in place to protect data is **not** there to create a **barrier** to sharing information. It exists to provide a framework to ensure that any personal and/or sensitive information is shared appropriately.

3. AIMS AND OBJECTIVES

Partner organisations and their officers need to feel confident of their obligations when requested, or requesting, to share information. The Framework aims to ensure compliance and consistency across the county by achieving the following objectives:

a) Creating a binding Framework to govern working practices and create greater transparency, data security and improved services for users
b) Offering guidance on how to share information lawfully
c) Increasing understanding of data sharing principles and legislation
d) Developing a template for Information Sharing Agreements to make it easier and quicker to formalise information sharing activities, ensuring risks are managed and providing assurance for staff and service users
e) Establish an efficient and reliable process to share information quickly
f) To protect partner organisations from allegations of wrongful use of data
g) To monitor and review information flows

By becoming a partner to this Framework, organisations are making a commitment to:

a) Apply the "Fair Processing" and "Best Practice" standards that are in the Information Commissioner's Data Sharing Code of Practice and checklists. See: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx
b) Adhere to, or demonstrate a commitment to achieving the appropriate compliance with the Data Protection Act;
c) Develop local Information Sharing Agreements that clearly and transparently demonstrate the reasons for sharing data and provide assurance on this activity.

4. GENERAL PRINCIPLES

This Framework recognises and promotes recommended good practice and legal requirements to be followed by all signatory organisations. This framework does not alter existing arrangements already in place for urgent sharing eg. related to child protection.

Systematic Information Sharing

Systematic information sharing involves routine sharing of data sets between organisations for an agreed purpose. Partner organisations who intend to share information systematically as a result of this Framework should complete an Information Sharing Agreement unless sector standards, for example, mean that an agreement is not required. If they are drawing up an agreement, they should use the Framework's approved Information Sharing Agreement Template to detail the specific purposes of the data sharing activity and have this signed off by their Senior Information Risk Officer (SIRO) or Caldicott Guardian as appropriate.

Partner organisations intending to share information, whether ongoing or as part of a time-limited exercise such as a project, should complete an Information Sharing Agreement using the approved template that sits under this Framework to detail the specific purposes of the data sharing activity and the responsibilities of participating organisations.

Ad-hoc Information Sharing

One off or ad hoc information sharing involves any exceptional sharing activities for a range of purposes which are not covered by routine data sharing arrangements. For ad hoc activities, an Information Sharing Agreement is not needed. Instead, the ad hoc information sharing checklist in the Guidance should be consulted to decide how to proceed, and advice sought from each organisation's Information Sharing contact where there is any doubt.

It is also good practice to record any ad hoc, one off data sharing activities detailing the circumstances, what information was shared and explaining why the disclosure took place. Remember, only share the minimum amount of data necessary and remove any fields or datasets which are not directly relevant before you share.

This Framework should be used in conjunction with local service level agreements and any other formal agreements between partner organisations, as well as existing Information Sharing Agreements.

All parties signed up to this Framework agree to be responsible for ensuring measures are in place to guarantee the security and integrity of data and that staff are sufficiently trained to understand their responsibilities and comply with the law. This document encourages sharing of data, but does not alter the statutory duties of those organisations signed up to it.

5. DATA SHARING AND THE LAW

Legislation gives information sharing its basis in law. The legislation listed below gives partners a mandate to share information as well as responsibilities for protecting information and preventing improper use. The main items of legislation regarding the use and protection of personal information are listed below and described in further detail in **Appendix C: Relevant Legislation**.

a) Data Protection Act (1998)
b) Human Rights Act (1998) Article 8
c) The Children Act (1989)

d) The Children Act (2004)
e) Civil Contingencies Act (2004)
f) The Common Law Duty of Confidence
g) Police Act (1996)
h) Crime and Disorder Act (1998)
i) Local Government Act (2000)
j) The Gender Recognition Act (2004)

Partner organisations must also be aware of any other legislation relevant to them when sharing specific information as this is not an exhaustive list of legislation.

The Freedom of Information Act 2000 (FOIA)

In addition to the legislation listed above, the FOIA gives everyone the right to request information held by public authorities and, unless exempt, to be told whether the information is held and be provided with the information.

Most, if not all, public sector bodies involved in data sharing are subject to the FOIA. This requires every public authority to adopt and maintain a publication scheme, committing them to publish information on a proactive and routine basis. In most cases this will include the policies and procedures relating to data sharing, including the details of the organisations with which data is shared and any relevant code of practice.

Any information shared between different partner organisations may be subject to an FOI request. Upon receipt of an FOI request the opinion of the originating party should be sought before decisions are made on whether to provide the information.

6. INFORMATION COVERED BY THIS FRAMEWORK

This Framework covers the closed sharing of a range of types of information, including personal, sensitive personal and business sensitive data. **Wherever possible, it is recommended that anonymised, aggregate or pseudonymised data is used to minimise the risk of any data protection breaches.** If you are in any doubt over whether you can share data and how to go about doing this, you should consult your organisation's Information Sharing contact.

Personal Information

Personal data refers to any data (manual, electronic, audio, visual and so on) which relates to a living individual (the data subject) who can be identified either from that data, or from any other information which is in the possession of, or is likely to come into the possession of, the data controller. (For the purposes of this framework, the data controller is the relevant partner organisation.)

Sensitive Personal Information

Sensitive personal data covers information which individuals would consider as private and would prefer to keep confidential. Additional conditions have to be met when sharing sensitive personal information. Examples of information considered as sensitive include:

a) the racial or ethnic origin of the data subject

b) political opinions
c) religious, or similarly held beliefs
d) membership of a trade union
e) physical or mental health conditions
f) sexual life
g) the commission or alleged commission of any crime

Anonymised Information

Any data which is anonymised can usually be shared without consent (subject to certain restrictions regarding health/social care records) provided the identity of the individual cannot be recognised.

However, organisations should ensure that anonymised data, when combined with other information from the same, or different sources, does not produce any information which can identify individuals, either directly or by summation.

There are several approaches to anonymisation and the appropriate approach will depend on the use to be made of the data:

- **Aggregation:** Aggregation of datasets about individuals into summary tables, so there are no longer rows relating to individuals.
- **Anonymisation:** Removal of identifiers in datasets at the level of individuals, so that there is no means to re-establish the link between the data and the individuals concerned.
- **Psuedonymisation:** Replacement of identifiers with alternative meaningless alphanumeric fields and reduction of potential identifiers to a partial form (e.g. year of birth instead of date of birth, partial post codes). If a set of keys is used to generate the alternative identifiers, then records relating to the same individual can be linked across datasets treated in the same way where research objectives require this.

Business Sensitive Information

Some information may be strategically or business sensitive, for example preparatory work around service redesign. Likewise, direct access to some datasets may need to be controlled because of licensing considerations preventing wider release. The loss, compromise or misuse of this type of information could cause serious damage to the organisation's reputation, or that of partners or lead to litigation.

7. ORGANISATIONAL RESPONSIBILITIES

Each organisation is responsible for ensuring that their organisational and security measures protect the information shared under this Framework.

General responsibilities include:

Ensuring that the information shared is necessary for the purpose for which you are sharing it, is shared only with those people who need it, is accurate and up-to-date, is shared in a timely fashion, and is shared, handled and processed securely. The Information Sharing Agreement provides these prompts before sharing takes place.

Considering the impact that decisions to share information may have on the individual, their safety and well-being and on others who may be affected by their actions.

Privacy statements to govern consent for information sharing should be compatible with the aims of this Framework to ensure that information can be shared within the terms of the consent given.

Partner organisations should independently or jointly ensure compliance with any Information Sharing Agreements they are involved in.

Organisations should consider making it a condition of employment that employees will abide by their rules and policies on the protection and use of personal and/or sensitive personal information.

Contracts with external service providers should include a condition that they abide by the relevant partner organisations' rules and on the protection and use of personal and/or sensitive personal information.

Incident reporting procedures should be in place which notify any other partners involved in the event of a breach of confidentiality or incident involving a risk or breach of the security of information.

Ensure that adequate security measures are in place to protect information – see **12. SECURITY** for more information.

Ensure that each Information Sharing Agreement establishes the arrangements for retention and disposal of information for all parties involved, including details of the exact arrangements for the storage and destruction of data where required.

Consent should be freely given and if a data subject withdraws consent to process their personal information (by serving a notice under section 10 of the Data Protection Act), other partners must be notified so that they can cease processing this data as soon as possible. Please note: certain exceptions exist which allow processing to continue. Contact your organisation's Information Sharing contact for more information.

Decisions about whether to share information or not and the reasoning behind them should be recorded. If you do decide to share information you should record exactly what data was shared, with whom and for what purpose.

Personal data responsibilities:

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

Staff should only be given access to personal data where there is a legitimate need, in order for them to perform their duties in connection with the services they are there to develop, deliver or monitor.

This Framework does not intend to give unrestricted access to information. Other organisations should only be able to access your data on a justifiable need to know basis and they should only allow relevant members of staff to access the data in order

to carry out their duties effectively. Access must be removed when it is no longer necessary.

Members of staff who will handle and share data within each organisation, including temporary, bank, contract or volunteer staff, should be trained so that they are aware of and comply with their responsibilities and obligations to maintain the security and confidentiality of personal information.

Information sharing must be compliant with relevant legislation as set out in **Appendix C** and with any other conditions partner organisations may attach in the Information Sharing Agreement they sign up to.

Personal data shall not be transferred to a country or territory outside the European Economic Area (EEA) without an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

Non-personal data responsibilities:

Partner Organisations should not assume that non-personal information is not sensitive and can be freely shared. In particular, anonymised data when combined with data from other sources may lead to individuals being identifiable. If you wish to share a partner organisation's data with a third party you must gain their consent.

Business/commercially sensitive data also requires protection against loss or corruption. The conditions on handling of these types of data will be in respect of the protective mark applied, or as otherwise set by the original data owner/controller, and in any case the partner organisation must be informed of any disclosure to a third party.

8. INDIVIDUAL RESPONSIBILITIES

Every individual working for the organisations listed in this Framework is personally responsible for the safekeeping of any information they obtain, handle, use and disclose and must be trained to carry out these duties.

Individuals are obligated to request proof of identity, or take steps to validate the authorisation of another before disclosing any information requested under this Framework and associated Information Sharing Agreements.

Every individual should uphold the general principles of confidentiality, follow the guidelines set out in the Cambridgeshire Information Sharing Guidance document and seek advice from their Information Sharing contact**.**

Individuals should be made aware that any violation of privacy or breach of confidentiality is unlawful and a disciplinary matter that could lead to their dismissal, and potentially, criminal proceedings. Partners should ensure that their HR teams support this process through effective induction/refresher training where necessary.

It is good practice to inform people how their data will be shared and exchanged between partner organisations. A public facing Charter in the form of a leaflet will be created in order to assist in explaining the information sharing process.

9. RESTRICTIONS ON USE OF INFORMATION SHARED

All shared information, personal or otherwise, must only be used for the purpose(s) specified at the time of disclosure(s) as defined in relevant Information Sharing Agreements unless obliged under statute or regulation, or under the instructions of a court or as agreed elsewhere. Any further uses made of this data will not be lawful or covered by the Information Sharing Agreement.

Secondary use of non-personal information may be subject to restrictions, i.e. commercial sensitivity or prejudice to others caused by the release of such information. If you wish to share information with a third party you should consult the information's original owner.

Certain information is subject to additional statutory restrictions, for example Criminal Records, HIV and AIDS, Assisted Conception and Abortion, Child Protection. Information about these will be included in relevant Information Sharing Agreements.

For advice on permission to share information you should approach your organisation's Information Sharing contact.

10. CONSENT – APPLIES TO PERSONAL DATA ONLY

The usual way to gain and control consent is through privacy statements or notices. These are written or oral statements given to individuals when information is collected about them and which cover, among other things: who is collecting the information, what will be done with it and who it will be shared with. These should be updated regularly to ensure that they remain relevant for your organisation and cover the information sharing activities you plan to undertake using them. For more detail, see the ICO's Privacy Notices Code of Practice.

Data subjects must have the right to withdraw consent at any time; if consent is withdrawn the organisation in question must inform partners as soon as practicable.

Personal data can be disclosed in certain circumstances without consent. This depends on certain 'Conditions for Processing' being met as defined in the Data Protection Act. Under the Data Protection Act, in order to disclose personal data at least one of the conditions listed in Schedule 2 of the Act must be met. In order to disclose sensitive personal data at least one condition in both Schedules 2 and 3 must be met. Contact your Information Sharing contact if you are in doubt.

When an organisation has a statutory obligation to disclose personal data the consent of the data subject (the person the data is about) is not required. However, where appropriate, the data subject should be informed such an obligation exists. In a case where a partner organisation decides not to disclose some or all of the personal data requested, the requesting authority must be informed.

Consent has to be signified by some communication between the organisation and the data subject. If the data subject does not respond, this cannot necessarily be assumed as implied consent. When using sensitive data, explicit consent must be obtained subject to any existing exemptions. In such cases the data subject's consent must be

clear and cover items such as the specific details of processing, the data to be processed and the purpose.

Specific procedures apply where the data subject is not considered able to give informed consent either because of the data subject's age (Fraser Guidelines) or where the data subject has a condition which means they do not have the capacity to give informed consent. Refer to the relevant partner organisation's policy on capacity to give consent under these circumstances.

Under certain circumstances, disclosures of information to another organisation may be justified when a relevant statutory exemption is met; these include:

- the prevention and detection of crime
- the capture or prosecution of offenders
- the assessment of collection of tax or duty

In cases where statutory exemptions do not apply you may still need to disclose personal information for safeguarding purposes if sharing the data would be in individuals' best interests.

11. INDEMNITY

Each partner organisation shall fully indemnify the other partner organisations and keep each of the other partner organisations fully indemnified against all claims, proceedings, actions, damages, costs, expenses and any other liabilities which may arise out of, or in consequence of, any breach of this agreement and in particular, but without limitation, the unauthorised or unlawful access, loss, theft, use, destruction or disclosure by the offending partner or its subcontractors, employees, agents or any other person within the control of the breaching partner organisation of any personal or sensitive data obtained in connection with this agreement.

12. SECURITY

It is assumed that each partner organisation has achieved or will aim to work towards information security standards such as ISO 27001, compliance with the NHS Connecting for Health Information Governance Toolkit or will adhere to a similar level of compatible security.

Partner organisations are encouraged to have an Information Security Policy in place to set out the minimum standards of security they require. Where partners do not have a specific policy in place the following principles should be followed:

a) Ensure that unauthorised staff and other individuals are prevented from gaining access to personal data.
b) Ensure visitors are received and supervised at all times in areas where personal data is stored.
c) Ensure computer systems containing personal data are password protected.
d) Passwords must be treated as private to the individual and must not be disclosed to others.

e) The level of security should depend on the type of data held, but ensure that only those who need to use the data have access.
f) Do not leave your workstation/PC signed on when you are not using it.
g) Lock away disks, tapes or printouts when not in use.
h) Ensure all new software has been authorised and disks are virus-checked prior to loading onto your PC.
i) Exercise caution in what is sent via email and to whom it is sent; and only transmit personal data by email where agreed compatible security arrangements are in place with partners (See **Appendix E: Government Secure Domains**).
j) If information is taken from system/s or network, ensure that appropriate security measures have been taken (eg. encryption).
k) Ensure the secure disposal of information (electronic and on paper).
l) Check that the intended recipients of faxes, emails and letters containing personal data are aware the information is being sent and can ensure security on delivery.
m) Ensure your paper files are stored in secure locations and only accessed by those who need to use them.
n) Do not disclose personal data to anyone other than the data subject unless you have the data subject's consent, or it is a registered disclosure, required by law, or permitted by a Data Protection Act 1998 exemption.
o) Do not leave confidential information on public display in any form. Clear your desk at the end of each day and lock sensitive material away safely.

Each partner signing this Framework agrees to adhere to these standards of security. Should additional security arrangements be required, these should be set out in individual Information Sharing Agreements as required.

It is the responsibility of the organisation which discloses personal data to make sure that it will continue to be protected by adequate security by any other organisations that access it by including clearly stated requirements in Information Sharing Agreements. Once the information has been received by the partner organisation they will have their own legal duties with respect to this information.

In the event of a security breach in which information received from another party is compromised, the originator will be notified at the earliest opportunity.

It is accepted that not all partners will have security classification in place, however, it is recommended that signatories to information sharing agreements: (i) protectively mark the materials they share to indicate the level of sensitivity, and (ii) align the protective marking classification they use with that used by Central Government. Further information is available from the Information Sharing contacts.

Participants in the Government Connect project will already be using this classification as it is a requirement for use of GCSx email accounts. Restricted, Protect, and Unclassified are the main markings relevant to information held by Local Authorities.

Information Sharing Agreements should be periodically reviewed to ensure that security arrangements are appropriate and effective.

13. INFORMATION QUALITY

Information shared should be complete (but not excessive), accurate and up-to-date to ensure all partners are assured that the information can be used for the purposes for which they require it. Organisations should also make any partners they share information with aware of their rules on data retention and whether these apply to the data being shared.

Organisations are expected to ensure that the personal and sensitive personal data they hold is processed in accordance with the Data Protection Act principles (see **Appendix C: Relevant Legislation)**.

14. TRAINING

Training must be provided for staff in all partner organisations who will have any duties handling or sharing information so that they can undertake their duties confidently, efficiently and lawfully. Each partner organisation must provide training and responsibility for this cannot be passed on to another organisation, although *delivery* of training can be passed on to a third party with that third party's consent.

To minimise the costs and ensure a consistent approach to training, it is advised that staff participating in a specific Information Sharing Agreement receive core training that has been jointly developed and is delivered by all parties who are sharing information under that agreement.

15. REVIEW ARRANGEMENTS

A cross-county Information Governance Monitoring Group will be established and will meet at least annually; with membership to be comprised of the specialists who act as each organisation's Information Sharing Point of Contact. The responsibilities of this group will be to:

- Review information governance procedures to establish whether they are still effective and working in practice.
- Monitor the effectiveness of the Information Sharing Framework and associated documents and update the contents when appropriate.
- Share best practice among partner organisations and update guidance to reflect this where necessary.
- Build a culture of information sharing between partner organisations by proactively communicating the aims of the framework
- Promote and implement education/training practices designed to encourage behaviour change in relation to information sharing.
- Support the development of Information Sharing Agreements under this Framework.

16. APPENDIX A: SIGNATORIES

Organisation	Chief Executive / Other	Date agreed
Cambridge City Council	Civic Affairs Committee	27 June 2012
Cambridgeshire Constabulary	Chief Constable Simon Parr	April 2012
Cambridgeshire County Council	Cabinet	17 April 2012 Agenda item 11
Cambridgeshire Fire & Rescue Service	Chief Fire Officer	CPSB on 28 February 2012 Reconfirmed 11 October 12
East Cambridgeshire District Council	Strategic Policy and Resources Committee	26 April 2012
Fenland District Council	Cabinet	19 April 2012
Hinchingbrooke Health Care NHS Trust	Jim O'Connell, Chief Executive Officer	Confirmed September 2012
Huntingdonshire District Council	Chief Officers Management Team	23 July 2012
NHS Cambridgeshire and NHS Peterborough	Governance and Compliance Committee	May 2012
South Cambridgeshire District Council	Cabinet	12 April 2012

17. APPENDIX B: KEY DOCUMENTS

Cambridgeshire Information Sharing…	Purpose	Hyperlink
• Framework	The umbrella agreement signed up to by the leaders of participating organisations. Sets out the standards that participating organisations will adhere to when sharing information.	http://data.cambridgeshire.gov.uk/data/information-management/info-sharing-framework/cambs-information-sharing-framework.pdf
• Guidance	Advice on how to identify when an activity is information sharing, and guidance on how the Framework can help with those activities. Good practice.	http://data.cambridgeshire.gov.uk/data/information-management/info-sharing-framework/cambs-information-sharing-guidance.pdf
• Agreement Template	Template for information sharing agreements under the umbrella of the wider Cambridgeshire Information Sharing Framework. Setting the parameters for specific information sharing activities between particular groups of organisations.	http://data.cambridgeshire.gov.uk/data/information-management/info-sharing-framework/cambs-information-sharing-agreement-template.doc
• Contacts	The lead information sharing officers in each participating organisation. Available to advise on the application of the framework and on information sharing more generally.	http://data.cambridgeshire.gov.uk/data/information-management/info-sharing-framework/cambs-information-sharing-contacts.doc
• Charter	A leaflet informing the public about Cambridgeshire's Information Sharing Framework and the benefits to them.	http://data.cambridgeshire.gov.uk/data/information-management/info-sharing-framework/cambs-information-sharing-charter.pdf

18. APPENDIX C: RELEVANT LEGISLATION

Your ability to share information is subject to a number of legal constraints and other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence. If you wish to share information, you must consider whether you have the legal power or ability to do so. This is likely to depend on the nature of the information in question and on who you are, and therefore what legislation applies to you.

Most public sector organisations derive their powers from statute. Before starting data sharing activities you should identify the relevant legislation for your organisation which defines the organisation's functions and the powers you may exercise in order to achieve your organisation's objectives. Broadly speaking, there are three ways an organisation may share data:

- **Express obligations** – where a public body is legally obliged to share particular information with a named organisation.
- **Express powers** – often designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".

- **Implied powers** – often legislation regulating public bodies is silent on data sharing. In these circumstances, it may be possible to rely upon implied powers to share information derived from express provisions in legislation. Express powers may allow organisations to do other things that are reasonably incidental to those which are expressly permitted.

Whatever the source of an organisation's power to share information, you must check that the power covers the disclosure in question – otherwise you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. For further information, consult your data sharing lead or legal services department. Also check whether there is a sector-specific guide addressing the information sharing you intend to undertake, such as the DWP's Guidance for Local Authorities on the use of social security data (2010).

The following list – which is not exhaustive – highlights legislation with particular relevance to guiding data sharing decisions.

a) Data Protection Act (1998) (DPA)

The Data Protection Act 1998 (DPA) governs the standards for processing personal data, including the collection, use of and disclosure of information. The legislation requires that data controllers meet certain obligations and it gives individuals certain rights with regard to their own personal data. The main standard for processing personal data is compliance with the 8 DPA principles listed below:

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 for any purpose or purposes 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 this Act.
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.

b) Human Rights Act (1998) (HRA) Article 8

The Human Rights Act enacts the European Convention on Human Rights in the UK. Article 8 of the Convention gives everyone the right to respect for his private and family life, home and correspondence, and is especially relevant when sharing personal data. Article

8 is not an absolute right - public authorities are permitted to interfere with it when it is lawful and proportionate to do so.

It is advisable to seek specialist advice if the disclosure or data sharing arrangement you are proposing is likely to have an impact on privacy which engages Article 8 or any HRA rights. If you disclose or share personal data only in ways that are compliant with the DPA, the disclosure of that information is likely to comply with the HRA. Personal data is normally exempt under the HRA.

c) The Children Act (1989)

Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Section 47 states that the authorities listed below must assist a local authority with enquiries of this nature by providing relevant information, unless doing so would cause more harm or be considered unreasonable:

- any local authority;
- any local education authority;
- any housing authority;
- any health authority; and/or
- any person authorised by the Secretary of State.

d) The Children Act (2004)

Section 10 of the Act places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant partner agencies to improve the well-being of children in their area in relation to:

- physical and mental health, and emotional well-being;
- protection from harm and neglect;
- education, training and recreation;
- making a positive contribution to society; and/or
- social and economic well-being.

e) Civil Contingencies Act (2004) (CCA)

In emergencies, it may be in the interests of affected vulnerable people for their personal data to be shared with emergency responders as defined in the CCA 2004. Sharing personal information may help emergency responders to perform statutory duties. The CCA 2004 1(1) defines an emergency as “an event or situation which threatens serious damage to human welfare and/or the environment or war or terrorism which threatens damage to security”. The principles and legislative provisions related to information sharing apply to the planning, response and recovery phases of emergencies.

f) The Common Law Duty of Confidence

The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are three categories of exception:

- Where there is a legal compulsion to disclose.

- Where there is an overriding duty to the public.
- Where the individual to whom the information relates consented.

Partners should consider which of these conditions are the most relevant for the purposes of an agreement. The guidance from the Information Commissioner states that because decisions to disclose 'in the public interest' involve the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking the decisions.

g) Police Act (1996) (PA)

Section 30(1) of the PA gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines these powers as powers under any enactment whenever passed or made. These powers include investigating and detecting crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.

h) Crime and Disorder Act (1998) (CDA)

Section 115 of the CDA confers a power on any 'relevant authority' to exchange information which is 'necessary' or 'expedient' to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder.

Section 17 CDA requires that all Local Authorities (LAs) consider crime and disorder reduction while exercising their duties. Sections 5 and 6 of the CDA impose a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area.

i) Local Government Act (2000) (LGA)

The main power specific to Local Authorities (LAs) is section 2 LGA (2000) – the power of "well-being". This enables LAs to do anything to promote social, economic, or social well-being in their area provided the act is not specifically forbidden by other statute. In addition, S111 LGA (1972) enables LAs to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place. The above are general powers for LAs but LAs have statutory powers relating to specific activities and these should be referred to as appropriate in any Information Sharing Agreements.

j) The Gender Recognition Act 2004 (GRA)

Under the Gender Recognition Act 2004 (GRA), individuals who have obtained gender recognition certificates (GRCs) in order to acquire legal status of their transitioned gender are entitled to legal protection from disclosure about their status. It is a criminal offence to disclose this status; ie. if someone has a gender recognition certificate stating they are a woman, it is a criminal offence to disclose that they used to be a man, except where explicit consent has been obtained from the individual involved or the disclosure is for the purposes of proceedings before a court or tribunal.

19. APPENDIX D: GLOSSARY OF TERMS

Anonymised information – information from which no individual can be identified.

Consent – The Information Commissioner's legal guidance to the Data Protection Act refers to the Directive, which defines consent as "…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Data controller – a person who (alone, jointly or in common with other persons) determines the purposes for which and the manner in which personal data is processed.

Data processor – any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Protection Act 1998 (DPA) – the main UK legislation which governs the handling and protection of information relating to living people.

Data sharing – the disclosure of data from one or more organisations to a third party organisation(s), or the sharing of data within an organisation. Sharing can take the form of systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and exceptional, one off decisions to share data for a range of purposes.
Data sharing agreements/Frameworks – set out a common set of rules to be adopted by the various organisations involved in a data sharing operation.

Duty of confidentiality – everyone has a duty under common law to safeguard personal information.

Personal data – data which relate to a living individual who can be identified—

a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy impact assessment (PIA) – is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of personal data.

Processing of data – in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including —

a) organisation, adaptation or alteration of the information,
b) retrieval, consultation or use of the information,
c) disclosure of information by transmission, dissemination or other methods

d) alignment, combination, blocking, erasure or destruction of the information.

Sensitive personal data – personal data consisting of information as to —

a) the racial or ethnic origin of the data subject,
b) his political opinions,
c) his religious beliefs or other beliefs of a similar nature,
d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e) his physical or mental health or condition,
f) his sexual life,
g) the commission or alleged commission by him of any offence, or
h) 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.

20. APPENDIX E: GOVERNMENT SECURE DOMAINS

Domains that are secure when used **end to end** for the exchange of data are:

x.gsi.gov.uk
gsi.gov.uk
gsx.gov.uk
gse.gov.uk
x.gcsx.gov.uk
.police.uk
.pnn.police.uk
.mod.uk
.cjsm.net
.scn.gov.uk
.nhs.net