Cambridgeshire and Peterborough Information Sharing Framework

Ratification Process

Lead Author	Information Sharing Framework Group
Developed by	Multi Agency IG Leads
Approved by	Organisation's IG Committees
Ratified by	Organisation's Boards
Version	2.5
Latest Revision date	April 2022
Review date	By April 2023 (or earlier if significant change to local or national requirements)
Valid on	April 2022

Document Control Sheet

Development and Consultation	Framework originally developed in 2012 by Cambridgeshire local authorities, Police, Fire and Rescue and Cambridgeshire and Peterborough Clinical Commissioning Group. This was also expanded to include health and social care delivered in the county by other partners including non-public sector partners.
Dissemination	This Framework will be promoted within the partner organisations on their own intranets with links to Cambridgeshire County Council's public website as a central point.
Implementation	A Caldicott Guardian/IG Lead in each organisation is responsible for monitoring the application of the Framework by ensuring that: - • The Framework is brought to the attention of all employees; • Appropriate training and guidance is provided to staff. • Communicated appropriately on intranets
Training	Training will be undertaken in line with the existing processes of each organisation
Audit	Implementation of the Framework will be monitored on a regular basis by IG Leads and the Cambridgeshire & Peterborough Information Framework Sharing Group.
Review	This Framework will be reviewed annually or earlier if there are changes in procedures or legislation.
Equality and Diversity	The Framework IG Group has carried out a Rapid Equality & Diversity Impact Assessment and no negative impacts were identified.

Revisions

Version	Page/Para No	Description of Change	Date Approved
2.1	Entire document	Complete document review and revision in accordance with GDPR/Data Protection legislation implementation 25 May 2018.	May 2018
2.2 2.3	various	Carry out final agreed changes	October 2018
2.4	Entire document	Complete document review and revision prior to circulation for agreement and sign up	July 2019
2.5	Entire document	Complete document review and revision prior to circulation for agreement and sign up	October 2021
2.6	Entire document	Complete document review and revision prior to circulation for agreement and sign up	April 2022

CONTENTS

THE FRAMEWORK

Public sector organisations in Cambridgeshire 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 and promote integrated working.

The Framework applies to all information being shared by and between 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.

IMPORTANT NOTE

Signing up to the framework does not mean that you can share information. It means your organisation has signed up to the principles and will abide by the standards it sets. You will still need an information sharing agreement which complies with our principles when created, agreed and reviewed.

The core member organisations are:

- Cambridge City Council
- Cambridge University Hospitals NHS Foundation Trust
- Cambridgeshire and Peterborough Clinical Commissioning Group
- Cambridgeshire and Peterborough NHS Foundation Trust
- Cambridgeshire Community Services NHS Trust
- Cambridgeshire Constabulary
- Cambridgeshire County Council
- Cambridgeshire & Peterborough Combined Authority
- Cambridgeshire Fire and Rescue Service
- East Cambridgeshire District Council
- Fenland District Council
- Huntingdonshire District Council
- North West Anglia Foundation Trust
- Peterborough City Council
- South Cambridgeshire District Council
- Royal Papworth Hospital NHS Foundation Trust
- East of England Ambulance Service Trust

Some organisations outside of the core membership have also signed up to the principles of the Framework. They are listed in **Appendix C: Affiliate Partners to the Framework.** Where an affiliate organisation wishes to join then a core member will sponsor this and Appendix D will be used to ensure that that organisations have appropriate information governance assurances. The sponsor will confirm that they have seen appropriate evidence.

Sharing with organisations who are not signatories to this Framework

Sharing information with an organisation who have not signed up to this framework is permitted. Care should be taken to ensure that the organisation is made aware of the principles in this framework, take account of existing relevant statutory frameworks and can provide evidence that they comply with data protection and there is an appropriate

agreement in place. Appendix D offers a checklist to ensure that organisations have appropriate information governance assurances.

INTRODUCTION

This Information Sharing Framework was developed to support information being shared appropriately and lawfully. 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 and Peterborough. The basis of the Framework is to provide guidance for partners to help share information in all appropriate situations to improve service delivery, planning and management 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 the overarching framework for the organisations that sign up to it. Any existing and subsequent 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 Legislation.

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.

AIMS AND OBJECTIVES

Partner organisations and their officers need to feel confident and knowledgeable 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 Framework to govern working practices and create greater transparency and data security allowing organisations to improve services in the delivery of care for those that need them.
b) Offering guidance on how to share information lawfully
c) Increasing understanding of data sharing principles and legislation
d) Developing, maintaining and using agreed templates for an Information Sharing Agreement and Data Protection Impact Assessment to make it easier and quicker to formalise information sharing activities, ensuring risks are managed and providing assurance for staff and service users
e) To create and maintain registers of sharing agreements and impact assessments to ensure that we do not duplicate work
f) Establish efficient and reliable processes to share information quickly
g) To protect partner organisations from allegations of wrongful use of data
h) To monitor and review information flows on an annual basis
i) Allow organisations to improve services for users and cooperate so they can deliver the care and services that those people with complex needs rely on
j) To provide the public with assurance that their data is managed in a secure manner and to assist the partner organisations in providing transparency in their handling of personal data.

By becoming a core member or affiliate member to this Framework, attendees and organisations are making a commitment to:

a) Demonstrate compliance with data protection legislation
b) Adopting ICO codes of practice and guidance on matters such as information sharing, impact assessment, anonymisation and pseudonymisation
c) Sharing knowledge, best practice and advice to other partners to help achieve success
d) Develop local Information Sharing Agreements and Data Protection Impact Assessments that clearly and transparently demonstrate the reasons for sharing data and provide assurance on this activity.

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 e.g. related to child protection.

Information sharing as part of a contract

This framework document and associated templates should not be used as substitute for a contract between controllers and processors. A contract should be used where a service is being provided on behalf of a controller. The contract should specify the information and purposes of processing and there should be no need for a separate information sharing agreement outside of that contract.

Systematic Information Sharing

Systematic information sharing involves routine sharing of data between organisations for an agreed purpose such as multi agency referral work. 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, or a contract is in place which provides for information sharing governance. If they are drawing up an agreement, they may 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.

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. This may be safeguarding or for the purposes of preventing or detecting crime. For ad hoc activities, an Information Sharing Agreement is not needed. Instead, advice should be sought from each organisation's IG lead on the appropriate form to use to record such sharing.

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 considered in conjunction with local service level agreements and any other formal agreements like contracts between partner organisations. .

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.

DATA SHARING AND THE LAW

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

- Data Protection Act 2018
- UK General Data Protection Regulation
- Freedom of Information Act 2000 and Environmental Information Regulations 2004

Human Rights Act 1998 Article 8

The following list is to guide but is not exhaustive and not all may apply in all cases:

- Children Act 1989
- Children Act 2004
- Civil Contingencies Act 2004
- Common Law Duty of Confidence
- Police Act 1996
- Crime and Disorder Act 1998
- Local Government Act 2000
- Gender Recognition Act 2004
- Care Act 2014
- Mental Health Act 1983
- Mental Capacity Act 2005
- Health and Social Care Act 2012
- Children & Families Act 2014
- Children and Young Persons Act 2008
- No Secrets, Department of Health 2000
- Criminal Justice Act 2003
- Privacy and Electronic Communications Act
- Safeguarding Adults, Association of Directors of Social Services 2005
- Working Together to Safeguard Children 2015 Statutory Guidance

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

ORGANISATIONAL RESPONSIBILITIES

Each organisation is responsible for ensuring that their organisational and security measures protect the information are sufficient to meet the requirements of data protection.

General responsibilities include:

- An individual with oversight of data protection
- A data protection policy available and disseminated to all staff
- Privacy Notices being made available
- Data Protection Impact Assessment process in place
- Contracts which contain appropriate data protection clauses
- Records of Processing Activity (ROPA) in place
- Training to staff provided
- Processes to enable the meeting of subject rights
- A policy in place to handle data breaches
- Identifying the appropriate lawful basis for processing information

What are the lawful bases for processing?

The lawful bases for processing personal information are set out in Article 6 of the UK GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. *(This cannot apply if you are a public authority processing data to perform your official tasks.)*

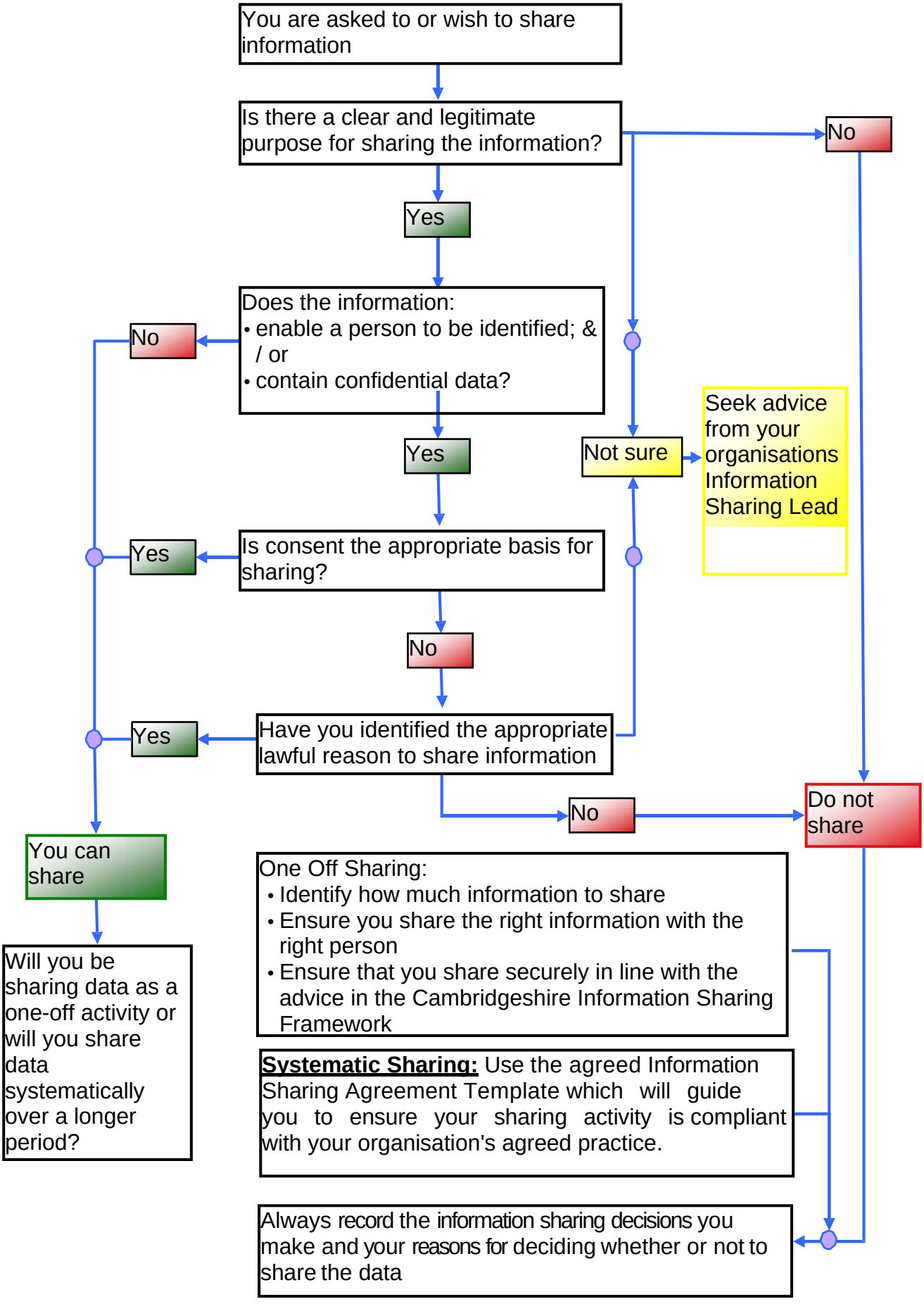
Article 9 of the UK GDPR sets out the bases for processing special category data and one of these must apply whenever you process special category data:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

If you are relying on conditions (b), (h), (i) or (j), you also need to meet the associated condition in UK law, set out in Part 1 of Schedule 1 of the DPA 2018.

If you are relying on the substantial public interest condition in Article 9(2)(g), you also need to meet one of 23 specific substantial public interest conditions set out in Part 2 of Schedule 1 of the DPA 2018.

Information Sharing flowchart



Further guidance is available from your Data Protection Officer and Information Governance Lead.

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 obliged 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 and follow the guidelines set out in their organisations policy documentation. They should seek advice whenever required from their Information Sharing contact - shown at Appendix A**.**

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 policies support this process through effective induction/refresher training where necessary.

It is good practice to inform people how their data will be used and shared between partner organisations. All partners will provide information for service users which sets this out and publish privacy notices as a minimum.

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.

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.

SECURITY

Each core member and affiliate partner will ensure that they attain and maintain information security standards such as:

- ISO 27001;

- being compliant with NHS Digital's Data Security and Protection Toolkit (formerly known as Information Governance Toolkit) or
- Public Services Network
- will adhere to a similar level of compatible security such as Cyber Essentials and any other security certifications.

Information Sharing Agreements will be reviewed at least annually to ensure that security arrangements are appropriate and effective.

BREACHES

If you have a data breach relating to an information sharing agreement, then you must make other signatories aware immediately and provide information on how this is being handled. Parties to an agreement under this framework will provide reasonable assistance to other parties where appropriate.

INFORMATION QUALITY

All organisations must put in place plans to carry out regular quality assurance across all teams that share data as part of an information sharing agreement.

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. Appropriate Information Governance training is mandated to be completed every year.

REVIEW ARRANGEMENTS

This framework will be reviewed by the Cambridgeshire & Peterborough Information Sharing Framework Group which will meet quarterly or at least bi-annually; with membership to be comprised of IG leads from each core member and affiliate members. These are detailed in Appendix A.

The aims and objectives of this group will be:

- Creating and maintaining a Framework to govern working practices and create greater transparency and data security allowing organisations to improve services in the delivery of care for those that need them.
- Offering guidance on how to share information lawfully
- Increasing understanding of data sharing principles and legislation
- Developing, maintaining, and using agreed templates for an Information Sharing Agreement or other documents such as Data Protection Impact Assessment to make it easier and quicker to formalise information sharing activities, ensuring risks are managed and providing assurance for staff and service users
- To create and maintain registers of sharing agreements and impact assessments to ensure that we do not duplicate work
- Establish efficient and reliable processes to share information quickly
- To protect partner organisations from allegations of wrongful use of data
- To monitor and review information flows on an annual basis

- Allow organisations to improve services for users and cooperate so they can deliver the care and services that those people with complex needs rely on
- To provide the public with assurance that their data is managed in a secure manner and to assist the partner organisations in providing transparency in their handling of personal data.

APPENDIX A: CORE MEMBERS

Organisation	Current Chief Executive / Accountable Officer	SPOC (DPO)
Cambridge City Council	Robert Pollock	Adam Brown Data Protection Officer
Cambridgeshire & Peterborough Clinical Commissioning Group	Jan Thomas	Amanda Holloway Data Protection Officer
Cambridgeshire & Peterborough NHS Foundation Trust	Tracy Dowling	Kay Taylor Information Governance Manager
Cambridgeshire Community Services NHS Trust (Including Peterborough Community Services)	Matthew Winn	Monty Keuneman Information Governance Manager
Cambridgeshire Constabulary	Nick Dean Chief Constable	
Cambridgeshire County Council	Stephen Moir	Ben Stevenson Data Protection Officer
Cambridgeshire Fire & Rescue Service	Chris Strickland Chief Fire Officer	Danielle Wilkinson
Cambridgeshire University Hospitals NHS Foundation Trust	Roland Sinker	Michelle Ellerbeck
East Cambridgeshire District Council	John Hill	Victoria Higham
Fenland District Council	Paul Medd	Amy Brown Data Protection Officer
Huntingdonshire District Council	Executive Leader – Cllr Graham Bull	Adam Brown Data Protection Officer
North West Anglia Foundation Trust (Formally Peterborough and Stamford Hospitals NHS Foundation Trust and Hinchingbrooke Health Care NHS Trust)	Caroline Walker	Sean Dykes
Peterborough City Council	Matthew Gladstone	Ben Stevenson Data Protection Officer
South Cambridgeshire District Council	Beverly Agass	Adam Brown Data Protection Officer
East of England Ambulance Service Trust (EEAST)	Robert Morton	Dean Ayres Acting IG Manager dpo@eastamb.nhs.uk
Royal Papworth Foundation Trust	Stephen Posey	Cath Willcox DPO

APPENDIX B: GLOSSARY OF TERMS

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

Consent – consent is a freely given and positive indication of that a person has chosen to allow their information to be used as described in a privacy notice or statement for example. It should not be a pre-condition to a service and they should have the ability to withdraw that consent. .

Data Controller – a person who (alone, jointly or in common with other persons) determines the purposes for which and the way 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.

UK General Data Protection Regulation and Data Protection Act 2018 (DPA) – the main UK legislation which governs the handling and protection of information relating to living people.

Data Protection Impact Assessment (DPIA) - is a means of assessing the risks to privacy and confidentiality associated with how personal data is being used.

Information Sharing – the disclosure of information by and between more than one organisation), 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 decision making to share data for a range of purposes.

Information Sharing Agreements/Frameworks – set out a 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.

- **a)** alignment, combination, blocking, erasure, or destruction of the information.

Special category 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.

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

APPENDIX C: AFFILIATE PARTNER SIGNATORIES

Other service providers signed up to the Framework principles include the NHS 111 Service and other Cambridgeshire and Peterborough Clinical Commissioning Group integrated working initiatives, they are associate members:

Organisation	Current Chief Executive / Accountable Officer	SPOC (DPO)
Herts Urgent Care	David Archer	Nick Cox
Queen Elizabeth Hospital Kings Lynn NHS Foundation Trust	Jon Green	Phil Cottis Head of Health Records and IG
East and North Herts CCG	Beverley Flowers	Sarah Feal
CGL Aspire		Mark Summerfield
Light Project Peterborough	Steven Pettican	
Cambridge Women's Resource Centre	Stef Martinesen-Baker	
Barnados		
HM Prison and Probation Service		
P3 Charity	Kate Greer	
Cross Keys Homes		

APPENDIX D: MEMBERS ASSURANCE

The following should be used to confirm the information governance assurances a member to the agreement can offer

Name of organization		
Data Protection Officer or Lead		Contact details
Name of organisation sponsoring this application:		
The below relate to the organisation seeking to become an affiliate member.		
Is the organisation registered with the ICO (please provide registration number)	Yes/No	Registration Number
Does this organisation provide health or social care services?	Yes/No	
Does the organisation complete the NHS DSP Toolkit? (if	Yes/No	ODS code
Does the organization hold Cyber Essentials certification?	Yes/No	Has certificate been seen?
Does the organization hold Cyber Essentials Plus certification?	Yes/No	Has certificate been seen?
Does the organization hold ISO27001 certification?	Yes/No	Has certificate been seen?
Does the organization have a current PSN certification?	Yes/No	Has certificate been seen?
If the answer all of the above, please describe what is in place to comply with data protection and information governance requirements including cyber security?		
The above is confirmed by:		
On behalf of applying organisation:		Date:
On behalf of Sponsoring organisation:		Date: