Portsmouth Information Sharing Framework 2019

Document Information	
Summary	Overarching framework which outlines the principles, standards of conduct and bases for using and sharing information by partner organisations working in Portsmouth.
Parties to the Agreement	Portsmouth City Council NHS Portsmouth Clinical Commissioning Group Portsmouth Hospitals NHS Trust Solent NHS Trust University of Portsmouth JobCentre Plus Hampshire Constabulary Hampshire Fire and Rescue. South Central and West Commissioning Support Unit
Date framework reviewed	December 2018
Date of next review	November 2021 (three yearly)
Agreement owners	Portsmouth Information Sharing Group
Agreement drawn up by	Portsmouth Information Sharing Group Contact: Alison Heywood, Partnership Information Governance Officer, Portsmouth City Council alison.heywood@portsmouthcc.gov.uk

Contents

Appendices

Foreword

Portsmouth has a long history of partner organisations working together to deliver better outcomes for citizens, employees and local businesses/employers as set out in The Portsmouth Local Strategic Partnership's Vision for Portsmouth:

Organisations represented on the Stronger Futures Board, Safer Portsmouth Partnership, the Health and Wellbeing Board as well as individual organisations working in Portsmouth are signed up to this Framework and are committed to promoting positive attitudes to information sharing to improve outcomes for individuals and to support each other in achieving the ambitions and aspirations we have for our city.

1. Introduction

1.1 This is an overarching framework which outlines the principles, standards of conduct and legal and justifiable basis for using and sharing information by partner organisations working in Portsmouth.

1.2 Partner organisations in Portsmouth need to share information so they can work effectively together to achieve better outcomes for Portsmouth citizens. Sharing information between partners helps us to:

- make decisions about plans to improve the city
- understand trends and patterns of activity so we can allocate resources more effectively
- respond to emergencies and disasters appropriately
- intervene at the right time and support the lives and safety of individuals, families and communities, and prevent and detect crime, apprehend and prosecute offenders, protect life and property, preserve order and
- fulfil our statutory duties and responsibilities.

1.3 Partners acknowledge their moral and statutory responsibility to share information carefully and responsibly and have developed the Framework to provide a common set of standards and conduct, to enable information to be shared fairly and lawfully and to promote their transparency and accountability.

1.4 As a city, we have considerable challenges to overcome in working together to achieve our vision, including:

- challenges arising from new and emerging models of public service delivery, such as integrated and multi-disciplinary services
- increased concerns about data security in more digitally enabled organisations and the need to address cyber security
- increased public awareness of privacy issues
- changes in the law concerning the protection of personal data with increased privacy rights for individuals
- the complex legal framework and widespread myths and uncertainty about the rules governing information sharing
- meeting our respective statutory responsibilities
- obtaining a balance between the need to share information to provide quality services and the protection of confidentiality.

1.5 The Portsmouth Information Sharing Framework aims to ensure that information is always shared in a legal and justifiable way that safeguards the individual.

1.6 Partners recognise that the duty to share information can be as important as the duty to protect confidentiality and will use the Framework to actively promote the sharing of information.

2. Aims and objectives of the Framework

2.1 The Portsmouth Information Sharing Framework ('the Framework') sets out the requirements which need to be addressed when sharing information so that partners can work together effectively.

2.2 Specifically, this Framework aims to support appropriate and necessary data sharing between organisations within Portsmouth and includes:

- the common purposes for holding and sharing information
- the general principles of information sharing
- the legal framework for sharing information
- sharing information without consent
- security of information.

2.3 It is expected that detailed information sharing agreements will be developed separately. These will specify what data is to be shared, how it will be shared and stored, to whom that data will be given for a particular area of activity and how it will be kept secure.

2.4 The Framework contains a number of templates which partner organisations can use for specific circumstances or projects, including data protection impact assessment and operational agreement templates. Any specific information sharing agreements developed by partners will comply with the principles and requirements contained in the overarching Framework. Responsibility for producing these specific information sharing agreements rests with the relevant partners.

2.5 Partners will promote information sharing and awareness of the Framework through appropriate communications media and develop local operational agreements for information sharing.

3. What does the Framework cover?

3.1 The Framework concerns the sharing of personal information i.e. information relating to an identified or identifiable person. Personal information may be anonymised or pseudonymised as a means of protecting an individual's identity

3.2 This Framework applies to all employees, elected members, non-executive members and trustees of partner organisations who agree to be bound by it.

3.3 Partners will abide by the Framework when sharing information with any other organisation or agency commissioned to deliver services on their behalf and will ensure that appropriate agreements and controls are in place, including in any commissioning arrangements, contracts or service level agreements etc.

3.4 The Framework is intended to complement the partners' respective professional codes of practice that apply to any profession working within the relevant organisation. The Framework does not constitute legal advice and partners should consult their Data Protection Officers and solicitors if they have concerns

about the legality of their information sharing. Matters may also be referred to the Portsmouth Information Sharing Group for discussion (see Appendix 1 for the Group's terms of reference).

4. Purposes for holding and sharing information

4.1 The common purposes for partners holding and sharing information include to

- develop evidence-led policies plan and commission more efficient, easier to access services
- improve existing and new services manage, report and benchmark performance promote accountability to customers, stakeholders, local residents and Government
- ensure that vulnerable children, young people and adults are protected
- allow organisations to cooperate so they can deliver the care and services that people need
- avoid duplication of data gathering
- monitor and protect public health and well-being
- audit accounts
- analyse statistics for research and teaching
- prevent and detect crime and promote community cohesion and safety
- investigate complaints or actual/potential legal claims
- plan for and respond to emergencies and civil contingencies across the city
- obtain civil orders for breach of tenancy obligations
- comply with legal responsibilities e.g. responding to court orders:

4.2 Partners will work together to maximise the benefits of sharing information for individuals and organisations by being better informed about their needs and being able to deliver more joined up services in order to:

- create a better experience for the service user, for example, individual may need to tell their story only once
- offer a single point of contact who acts in a coordinating role on behalf of the partner organisations,
- support the use of case management approaches and help to prevent organisations working in conflict with one another
- provide support that is more tailored to the needs of the individual
- identify underlying problems as well as inter-related problems
- ensure better targeting of services and better identification of who might help
- be able to be preventative and more proactive, thereby being better placed to avoid crisis points
- exploit the efficiencies and financial benefits and the ability to manage demand.

4.3 Partners may wish to share information about people with complex needs such as mental health and substance misuse, so that people get the most appropriate service when they experience more than one problem at the same time.

4.4 Partners may wish to share information to ensure that individuals receive timely support to prevent their needs from escalating.

> An example of this is the Multi-Agency Safeguarding Hub (MASH) where co-located partners from the police, local authority and community nursing services are able to share information immediately between a range of agencies so that more appropriate decisions can be made quickly about referred cases.

4.5 Partners may share information to understand the needs of individuals and the local population**,** plan the delivery of services and demonstrate their impact.

> An example of this is the Troubled Families Programme in Portsmouth where the local authority relies on access to data and intelligence on families and family members held by partner organisations. Without sharing this information, there is a risk that families with the highest need will not be identified and will not receive the coordinated support they need.

4.6 Partners may share information to protect children, families and adults at risk of abuse and neglect and to learn from past lessons. By discussing individual cases and reflecting on information sharing practice, partners can improve the way children, families and adults at risk are protected and help to prevent a family reaching the point of crisis and improve outcomes for individuals.

> An example of this are the Portsmouth City multi-agency teams (MAT) operational and network meetings 'Team Around the Worker' approach whereby practitioners discuss cases involving young people and/or families where guidance or reflection would be helpful and or cases that the worker has found distressing or where learning from a specific incident would be helpful.

5. Principles underpinning this Framework

5.1 Partners agree to abide by the Seven Golden Rules for data sharing about individuals (Appendix 2) and the Seven Golden Rules about systematic data sharing (Appendix 3)

5.2 Health and Social Care Partners will share health and social care information in accordance with The Caldicott Principles (Appendix 4)

5.3 Information will be shared where there is a legal basis to do so and in accordance with prevailing legislation (see Legal Framework, Appendix 5). The relevant bases and purposes for sharing will be identified within the specific information sharing agreements.

5.4 Where the provision of anonymised or pseudonymised data is adequate, partners will use these as a preferred method in accordance with the Information Commissioner's Office Anonymisation Code of Practice. https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

5.5 Partners will ensure that information is shared or requested on a justifiable ‘need to know’ basis. Only such data as is relevant for the purpose for which it is disclosed will be shared by partners.

5.6 Partners will abide by the following principles of the Framework:

1. To work together to promote information sharing and to overcome barriers to sharing information
2. To be transparent in the way they share information
3. To share information with each other where it is lawful
4. To use anonymised or pseudonymised data where this is adequate and appropriate
5. To adopt a 'privacy by design approach and ensure that data protection is a key consideration in the early stages of any project or programme
6. To ensure the security of personal data by applying adequate technical and non-technical security measures to the personal data they hold and transfer.

Principle 1. Partners will work together to promote information sharing and to overcome barriers to sharing information.

Partners recognise the benefits of sharing information and the adverse impacts of not sharing information for individuals and for their organisations and agree to work together to address the cultural, technical and organisational barriers to sharing information.

Principle 2. Partners will be transparent in the way they share information.

Partners will work together to meet their respective requirements to be more transparent in the way they handle and share information. Fair processing or 'privacy 'notices should be in place at the point of collection and will explain the purposes of collecting information, who will see it and who it is shared with, as well as the individual's rights of access (see the ICO Privacy Notice Code of Practice). https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

Young people and adults at risk will be given specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.

Principle 3. Partners will share information where it is lawful.

Partners involved in providing services to the public have a responsibility to ensure that their use of personal information is lawful, properly controlled and that the individual's rights are respected.

Information sharing agreements will specify the legal basis on which any personal data may be shared with partner organisations and detail any particular legal obligations requiring personal information to be shared. https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

Principle 4. Partners will use data in a form where identification is not likely to take place unless it is necessary to identify individuals

It can be beneficial to join partners' information, to inform the way services are planned and commissioned by partner organisations, for example, to develop more integrated services and to make best use of partners' resources

There is a general expectation, that anonymised data will be used for planning purposes and for carrying out research.

Partners will take suitable steps to ensure that anonymisation is conducted effectively and lawfully, in accordance with the ICO Anonymisation Code of Practice, to prevent individuals from being identified or re-identified

https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

Where personal information cannot be suitably anonymised, then consent will need to be sought from the individual or another legal basis found.

Principle 5. Partners will adopt a 'privacy by design' approach

Partners will adopt a 'privacy be design' approach by ensuring that privacy and data protection is a key consideration in the early stages of any project or programme, and throughout its lifecycle. For example when:

- building new IT systems for storing or accessing personal data;
- developing legislation, policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using information for new purposes.

Partners recognise their statutory responsibility to carry out a Data Protection Impact Assessment on the use of personal data considered 'high risk, for example, when undertaking large scale processing of 'special categories' of personal information (sensitive information) or setting up automated processes.

A Data Protection Impact Assessment will be completed before developing an information sharing agreement in order to consider the potential risks and solutions in connection with the collection, use and sharing of information. Partners agree to work together to complete the relevant DPIA template to the standard required by data protection legislation and the ICO (see the ICO's Data Protection Impact Assessment Guidance.

Principle 6. Partners will ensure the security of personal data

Partners shall have appropriate technical and organisational measures in place to protect the confidentiality, integrity and availability of the data during all stages of processing. It is envisaged that each party will adhere to common standards for data security.

Each party shall have formal procedures to:

- Ensure the security of personal data before, during and after data sharing takes place.
- Deal with breaches or suspected breaches of legislation or other duty, stated or implied, relating to the confidentiality of personal data, including measures for co-operation between the parties to the Framework.

Where organisations use a security classification scheme (such as the Government Security Classification Policy), it is the responsibility of those organisations to apply the appropriate level of security and use of protective marking when they are sharing information. Partners should refer to local guidance on security classification if they require further guidance.

6. Legal framework for sharing information

6.1 The legal framework within which partner organisations share information is complex and overlapping and there is no single source of law that regulates public sector data sharing. The principal laws, regulations and guidance are:

- the Common Law Duty of Confidence
- the Human Rights Act 1998
- the Data Protection Act 2018 and General Data Protection Regulation 2016
- the ICO Data Sharing Code of Practice and Data Sharing Checklists

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

7. Lawful bases for sharing information

7.1 Personal data may be shared where it is necessary to comply with a legal obligation to which a partner may be subject or some other legitimate basis laid down by law (see Appendix 5). Where no such legal avenue exists, partners will gain informed consent from the individual.

7.2 In deciding whether or not sharing of information given in confidence is justified it is necessary to weigh the harm that would result from breach of confidence against the harm that might result if you fail to disclose the information.

7.3 The decision to disclose under these circumstances must be documented and include the reason for the decision, who made the decision, who the data was disclosed to and the date. A decision not to share data should also be recorded.

7.4 Partners should contact their organisation's Information Governance Team, Data Protection Officer or seek legal advice if they are unsure about whether it is lawful to share personal data. Where the legal basis for disclosing information is disputed, the matter should be referred to the Caldicott Guardian (for health and social care services) or Senior Information Risk Owner (SIRO) of the relevant partner organisation/s for resolution.

8. Sharing information on the basis of consent

8.1 Where partner organisations rely on the consent of the individual as the basis for sharing their information, they must be able to demonstrate that it was freely given, specific, informed and unambiguous for each purpose for which the data is being shared.

8.2 Consent will not be regarded as freely given if the individual has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

8.3 Where consent is required, permission to share information should be obtained from the individual at the start of their involvement with partners' services. Partners will obtain explicit consent from individuals to share their personal information with partners and with people and organisations, including sharing information with multi-agency and integrated services and put in place suitable arrangements for managing any objections.

9. Partners' responsibilities

9.1 Partners who sign up to this Framework are responsible for embedding this Framework within their own processes relating to information sharing. Partners who share information under this Framework will:

- ensure staff are aware of and comply with their responsibilities and obligations with regard to the confidentiality of personal data about people who are in contact with their agency
- know who to contact, and processes to follow, in the event of a breach of confidentiality
- ensure the commitment of the organisation to share data legally and within the terms of an agreed specific information sharing agreement
- ensure the commitment that data will only be shared on a need-to-know basis and on the understanding that disclosure of personal data which cannot be justified, whether intentionally or unintentionally will be subject to disciplinary action, and maybe subject to legal sanctions.

9.2 Partners will ensure information disclosed is recorded appropriately by:

- ensuring that all personal information that has been disclosed to them under an agreement is recorded accurately on that individual's manual or electronic record in accordance with the agency's policies and procedures
- putting in place procedures to record the details of the information shared, the provider and who received the information.

10. Data quality

10.1 Data shared should be of a good quality and it is recommended that the data shared follows either the Audit Commission's six principles of data quality, or other appropriate guidance used by the organisations sharing the data. The six data quality principles are:

- accuracy
- validity
- reliability
- timeliness
- relevance, and
- completeness.

10.2 Further information about these principles can be found in the Audit Commission document entitled "Improving information to support decision making: standards for better quality of data.

10.3 Organisations must ensure that individuals are aware of their personal responsibilities with regard to ensuring the quality of personal data, and who individuals should contact if queries arise.

11. Access to data

11.1 Partners will ensure that their employees and contractors will only have access to the information they need in order to carry out their particular role.

11.2 Any third party access (i.e. users who are not employed by the partner organisation) to partners' data and information systems will be based on there being a clear business case and legal justification for sharing information about the individual(s) concerned. Access will be given to the relevant partner's records as deemed necessary by the owning partner for external organisations' employees to carry out their work relating to the specific role and purpose for which access has been granted and on meeting the owning partner's conditions of access.

11.3 Individual Information Sharing Agreements will provide more detail of information to be shared, access to records and systems and the associated controls around their use and management.

12. Rights of data subjects

12.1 Partner organisations acknowledge a duty to assist one another in meeting their individual responsibilities to provide information in response to data subject access requests and in addressing other rights of data subjects, including rights to have inaccurate records corrected and, in certain circumstances, to have information erased.

12.2 Partners will assist one another in addressing the rights of data subjects to be informed about how their personal data may be shared and in ensuring that suitable privacy notices are made readily available at the point of collecting personal data.

13. Retention and disposal

13.1 Partners agree that personal data will not be held for longer than necessary to fulfil the purpose for which it was collected and will be disposed of securely in accordance with national guidance and each organisation's local information retention and disposal policy.

14. Information sharing agreements

14.1 Agreements set out how partner organisations will meet their respective duties when processing and sharing personal data.

14.2 An information sharing agreement alone does not allow personal data to be processed or shared, but it can help partner organisations ensure that there are suitable arrangements in place to share personal data fairly and lawfully and to comply with other legal requirements for handling data.

14.3 Information sharing agreements can also be used to demonstrate compliance to supervisory bodies, including the Information Commissioner's Office and together with any relevant privacy notices, provide details to the public about how partner organisations share personal information with one another.

14.4 Information sharing agreements will be supported by a data protection impact assessment. The agreements can include controls for mitigating potential risks arising from sharing personal data identified through the data protection impact assessment.

14.5 Information sharing agreements should take account of the principles and commitments that organisations will adopt when processing or sharing personal data and provide details of the following:

- the Parties to the Agreement
- the data being processed or shared, including details of special categories of personal data
- the reason or purpose for processing and sharing the data
- the identity of the data controller/s and data processors, their roles and their responsibilities
- the lawfulness of the data processing and sharing and the specific conditions under the legislation for processing sharing personal data
- consent arrangements (where consent is used as the legal basis for sharing) and details of how any objections will be handled
- how individuals will be told their information will be shared (e.g. fair processing or privacy notice or statement)
- roles and responsibilities of staff in each organisation and details of Data Protection Officers for each of the parties to the agreement
- security (the technical security measures that will protect personal data and the systems that will be put in place to maintain security)
- who will have access to the data and the level of access agreed
- data quality
- requests for information and how these will be handled
- review arrangements

14.6 Partners will work together to complete the relevant information sharing agreement templates to the standard required by data protection legislation and the ICO (see the ICO Data Sharing Code of Practice).

14.7 Partner organisations wishing to put a new operational agreement in place should follow the steps below:

1. As early as possible, contact your organisation's Information Governance (IG) lead to check whether there is an existing protocol/agreement you could use. If not, seek advice and/or help with the process.
2. Ensure that the same discussion is taking place at the agency with which your organisation needs to share data.
3. Establish your legal justification for sharing this data (see Appendix 5 of this document).
4. Forward the draft PIA to the organisation/agency with whom you wish to share data to check and ensure that they and their IG lead are happy with the assessment and agreement.
5. Each organisation must have a data protection impact assessment ratified and signed by an authorised signatory – usually a senior manager with responsibility for IG e.g. the Data Protection Officer and Caldicott Guardian or Senior Information Risk Owner (SIRO).

6. Develop the draft operational agreement (OA) to the organisation/agency with whom you wish to share data to check and ensure that they and their IG lead are happy with the agreement.
7. Finalise the OA for signing by the relevant data owners in the partner organisation.
8. Add the OA to partner organisations' information sharing agreement registers
9. Publish a summary on the Portsmouth Information Sharing Framework website.
10. Review and update the agreement.

An operational agreement for data sharing template is included at Appendix 6 as an example

15. Sharing information for research purposes

15.1 Information is essential to support the provision of services, including where partner organisations need to work closely together to plan and deliver services. It is also essential to improve the quality and effectiveness of those services and to support innovation, for example through research.

15.2 It can be particularly beneficial to join partner organisations' information to inform the way services are commissioned, to develop more integrated services and to make best use of partners' resources

15.3 Any use of personal information for research and related purposes has to be compliant with confidentiality and data protection law. There is a general expectation, therefore, that anonymised data will be used for research and planning purposes. Care should be taken when using anonymised data to prevent individuals from being re-identified, in accordance with the ICO Anonymisation Code of Practice

https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf

15.1 Where personal information cannot be suitably anonymised, then consent will need to be sought from the individual or another legal basis found for using personal information for research purposes. Whilst there are exemptions under the Data Protection Act that allow the use of data collected for one purpose to be used for research purposes. Care should be taken in applying these exemptions to ensure that they meet the necessary conditions for exemption. Advice should be sought from information governance and research governance or ethics committees (where relevant) ahead of undertaking research requiring the use of personal data.

15.2 There are complex rules around linking and sharing personal information for purposes other than for direct care, including the use of NHS numbers and pseudonymised data to do this. Any data matching or linking and analysis using NHS data should be carried out using approved NHS frameworks supported by a Data Protection Impact Assessment and Data Processing Agreement.

15.3 Partner organisations need to be transparent in the way and explain through privacy notices and other privacy information any uses of personal information for research purposes, including where this data is anonymised

16. Sharing with organisations who are not signatories to this Framework

14.1 If it is necessary to share data with an organisation who is not party to this overarching Framework, consideration should be given on a case by case basis as to whether or not a data protection impact assessment is required and whether a specific information sharing protocol and agreement should be put in place for that information flow.

17. Monitoring and review

15.1 The Portsmouth Information Framework Group will, in conjunction with partner organisations, review this overarching Framework three yearly unless new or revised legislation necessitates an earlier review. Each partner organisation will be individually responsible for monitoring and reviewing the implementation of the Framework and any individual Information Sharing Agreements they may have.

18. Breaches

16.1 All agencies who are party to this Framework will have in place appropriate measures to investigate and deal with the inappropriate or unauthorised access to, or use of, personal data whether intentional or unintentional.

16.2 In the event that personal data shared under this Framework is or may have been compromised, whether accidental or intentional, the organisation making the discovery will, without delay:

- take appropriate steps, where possible, to mitigate any impacts;
- inform the organisation who provided the data of the details;
- take steps to investigate the cause;
- take disciplinary action against the person(s) responsible, if appropriate;
- take appropriate steps to avoid a repetition.

16.3 On being notified of a breach, the original data provider along with the organisation responsible for the breach, and others as appropriate, will assess the potential implications for the individual whose data has been compromised, and if necessary will:

- notify the individual(s) concerned;
- advise the individual(s) of their rights; and
- provide the individual(s) with appropriate support.

16.4 Where a breach is identified as serious, it may have to be reported to the Information Commissioner's Office. The original data provider, along with the breaching organisation and others as appropriate, will assess the potential implications, identify and agree appropriate action.

19. Complaints

19.1 Partner organisations must have in place procedures to address complaints relating to the disclosure of data. The partner organisations agree to cooperate in any complaint investigation where they have data that is relevant to the investigation. Partners must also ensure that their complaints procedures are well publicised.

19.2 If the complaint affects more than one partner organisation it should be brought to the attention of the appropriate complaints officers who should liaise to investigate the complaint.

Appendix 1. Portsmouth Information Sharing Group Terms of Reference

Portsmouth Information Governance Group

Terms of Reference September 2017

1 Purpose

The Portsmouth Information Sharing Group is responsible for developing, co-ordinating and delivering the Information Sharing Framework and associate resources for agencies working in Portsmouth and for actively promoting the sharing of information through this Framework for the benefit of the community.

2 Relationships

The Information Sharing Group will report on developments and progress to the Portsmouth Health and Social Care Executive twice a year and at other times by exception. The Partnership boards in the city also have a direct interest in ensuring that the Information Sharing Framework is in use and is fit-for-purpose.

3 Remit

1. Ensure the Framework and associated resources are up-to-date and accurate in terms of legislation and good practice, and meet the needs of partner agencies

2. Monitor 'sign-up' to the Framework

3. Maintain list of all Operational Agreements and publish examples on webpage (http://www.portsmouth.gov.uk/living/27521.html)

4. Share good practice and updates on legislation

5. Identify and resolve any cross-agency communication issues

6. Help partner agencies to resolve any information sharing issues

7. Review the Framework every two years or when major changes are needed.

8. Debate problems associated with developing and implementing the Framework, and identify solutions.

9. Panel members will:

- Contribute resources towards Framework products from their own areas of expertise and/or Service/organisation
- Actively promote and embed Framework and resources within their own organisation
- Communicate issues to/from the Panel/own organisation

10 Escalate resourcing and any other issues to the Portsmouth Health and Social Care Executive and to their respective Information Governance Boards for resolution

4 Membership

Membership is drawn from organisations in Portsmouth which have agreed to be party to the Information Sharing Framework. Members will usually be specialists in information governance. At October 2012, the relevant organisations comprise:

- Portsmouth City Council
- NHS Portsmouth/Clinical Commissioning Group
- Portsmouth Hospitals NHS Trust
- Solent NHS Trust
- University of Portsmouth
- JobCentre Plus
- Hampshire Constabulary
- Hampshire Fire and Rescue.

5 Meetings

5.1 The Group will meet twice a year, and by exception at other times to discuss and resolve any urgent issues. Representatives will include will include IG leads and strategic managers from the Information Sharing Framework member organisations.

5.2 The agenda will be set by the Chair and circulated by the Partnership IG Officer one week before the meeting

5.3 Items for inclusion on the Group's agenda should be forwarded at least one week before the meeting.

6 Review date

September 2018

Contact:

Alison Heywood

Partnership Information Governance Officer, Portsmouth City Council

alison.heywood@portsmouthcc.gov.uk

Appendix 2

Seven Golden Rules of data sharing on an individual basis

1. Remember that the Data Protection Act is not a barrier to sharing data but provides a framework to ensure that personal data about living persons is shared appropriately

2. Be open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom data will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.

3. Seek advice if you are in any doubt, without disclosing the identity of the person where possible.

4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential data. You may still share data without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgment on the facts of the case.

5. Consider safety and well-being: Base your data sharing decisions on considerations of the safety and wellbeing of the person and others who may be affected by their actions.

6. Necessary, proportionate, relevant, accurate, timely and secure: Ensure that the data you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely.

7. Keep a record of your decision and the reasons for it - whether it is to share data or not. If you decide to share, then record what you have shared, with whom and for what purpose.

   Information Sharing: Guidance for Practitioners and Managers

   HM Government, March 2009

Appendix 3

Data sharing checklist for systematic data sharing

(i.e. where you are entering into an agreement to share personal data on an ongoing basis)

Is the sharing justified?

Key points to consider:

• What is the sharing meant to achieve?

• Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?

• Is the sharing proportionate to the issue you are addressing?

• Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

• The type of organisation you work for.

• Any relevant functions or powers of your organisation.

• The nature of the information you have been asked to share (for example was it given in confidence?).

• Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

As well as considering the key points above, your data sharing agreement should cover the following issues:

• What information needs to be shared.

• The organisations that will be involved.

• What you need to tell people about the data sharing and how you will communicate that information.

• Measures to ensure adequate security is in place to protect the data.

• What arrangements need to be in place to provide individuals with access to their personal data if they request it.

• Agreed common retention periods for the data.

• Processes to ensure secure deletion takes place.

Source: ICO Data Sharing Code of Practice Data Sharing Checklists

Appendix 4

The Caldicott Principles

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix 5 Legal framework

The Common Law Duty of Confidence

An obligation of confidence will exist where the individual has provided the information to another in circumstances where it is reasonable to assume that the provider of the information expected it to be kept confidential. Where there is a clear duty of confidence the information can only be disclosed to “third parties” if there is informed consent, compulsion of law or public interest.

The Human Rights Act 1998

Sharing information will comply with the HRA if it:

(a) is made for the purposes of preventing crime, protecting the health and/or safety of alleged victims and/or the rights and freedoms of those who are victims of domestic violence and/or their children;

(b) is necessary for the purposes referred to in (a) above and is no more extensive in scope than is necessary for those purposes; and

(c) complies with all relevant provisions of law.

The EU General Data Protection Regulation (GDPR) 2016

The GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject **(the 'lawfulness, fairness and transparency' principle)**

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes **(the 'purpose limitation' principle)**

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed **(the 'data minimisation' principle)**

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **(the 'accuracy' principle)**

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed **(the 'storage limitation' principle)**

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures **(the 'integrity and confidentiality' principle)**

<u>Sharing personal data</u>

The GDPR will allow for **personal data** to be shared if:

(a) The data subject gives their consent

(b) Sharing is necessary for the performance of a contract with the data subject

(c) Sharing is necessary for compliance with a legal obligation

(d) Sharing is necessary to protect the vital interests of a data subject or another person

(e) Sharing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

(f) Sharing is necessary for the purposes of legitimate interests pursued by the controller or a third party

Sharing personally sensitive data

The GDPR also identifies **special categories of personal data** (referred to in the Data Protection Act as 'sensitive data') and these can be shared if:

(a) The data subject gives their **explicit** consent

(b) Sharing is necessary for carrying out obligations under employment, social security or social protection law

(c) Sharing is necessary to protect the vital interests of a data subject or another individual (where the data subject is physically or legally incapable of giving consent)

(d) The data subject has already made the information public

(e) Sharing is necessary for the for the purpose of a legal claim or where courts are acting in their judicial capacity

(f) Sharing is necessary for reasons of substantial public interest

(g) Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services where this is required by law or a contract with a health professional

(h) Sharing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

(j) Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

Personal data' means any information relating to an identified or identifiable person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, 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 data are defined as 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

The Data Protection Act 2018

The Data Protection Act 2018 Act makes provisions for how the GDPR applies in the UK. It is therefore important the GDPR and the DPA 2018 are read side by side. Schedule 1 of the Act, for example, provides a list of conditions which, if one is met, permit the processing of the special categories of personal data and criminal conviction data.

The new Act also contains law enforcement provisions in response to the EU Data Protection Directive 2016/680.

Other legislation concerning sharing personal data

The following legislation requires public authorities to share specific information in certain prescribed circumstances and may provide partner organisations with a legal basis for sharing personal data.

- NHS (Venereal Diseases) Regulations 1974
- Notifications of Births and Deaths Regulations 1982
- Codes of Practice, Mental Health Act 1983, s 1.3 – 1.13 and s 14
- Police and Criminal Evidence Act 1984
- Public Health Act 1984
- Public Health (Infectious Diseases) Regulations 1998
- Children's Act 1989 s 47
- Abortion Regulations 1991
- Finance Act 1994
- VAT Act 1994, s 91
- Criminal Procedure Investigation Act 1996
- Social Security Administration (Fraud) Act 1997
- Audit Commission Act 1998
- Crime and Disorder Act 1998, s 115
- Terrorism Act 2000 s 19
- Civil Contingencies Act 2004.
- the Children Act 1989 and 2004
- the Crime and Disorder Act 1998
- the Health and Social Care Act 2012
- the Health and Social Care Act (Quality and Safety) 2015
- the Care Act 2014
- the Children and Families Act 2014
- Regulatory Investigatory Powers Act 2000
- Police Reform Act 2002
- Criminal Justice Act 2003
- Civil Contingencies Act 2004
- Safeguarding Adults, Association of Directors of Social Services 2005
- Housing Act 1989

- Police and Justice Act 2006
- Guidance on the Management of Police Information 2010
- Working Together to Safeguard Children 2015 Statutory guidance
- Local Government & Public Involvement in Health Act 2007
- Children and Young Persons Act 2008.

Appendix 6. Example Operational Agreement for Data Sharing Template

Operational agreement for data sharing *[insert name of partner organisations and project title/purpose for data sharing]*

Start date:

Review date:

Document Control Sheet

Version	
Status	
Authors	
Date Created	
Date Last Updated	

Operational agreement for data sharing

Scope and purpose

This is an Operational Agreement (OA) for data sharing between *[insert names of the partner organisations who will be parties to the agreement].*

This OA covers the exchange of data between the Parties, *[insert name of partner organisation who will be sharing data]*. It supports the organisations involved and the people it impacts upon. It details the specific purposes for sharing and the personal data being shared, the required operational procedures, consent processes, and legal justification that underpins the disclosure/exchange of data.

Privacy impact assessment

A privacy impact assessment has been completed to determine whether the new information sharing project or process presents any privacy concerns and to ensure the Parties comply with their data protection obligations and meet individuals' expectations of privacy.

Any privacy risks identified have been addressed in this Operational Agreement

Definitions and interpretations

In this agreement:-

- *['the Council' means Portsmouth City Council of Civic Offices, Guildhall Square, Portsmouth, PO1 2LA]*
-

[insert details of partner organisations who will be sharing data and define any key terms used in the agreement]

Objectives

The objectives of sharing the data covered by this agreement are

[Insert details here in bullet point form of the objectives of the data sharing covered under this agreement.]

•

Individuals impacted by this OA

The residents/clients/service users and/or carers which this OA relates to include:

[Insert details of the residents in bullet point form here].

•

The benefits to the people include:

[Insert details here in bullet point form of how the OA will benefit residents].

•

Data to be shared

Only the **minimum necessary** personal data consistent with the purposes set out in this document must be shared. The data to be shared consists of:

[Describe or list data to be shared. If possible include a full list of data items to be shared here or enclose as an appendix to the agreement]

Legal justification for sharing

The partners will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

Where personal data will be shared under this agreement, there must be a legal justification to allow the sharing (see appendix 1 for the legal framework and justifications for sharing personal data).

The partners, when acting as a Controller, will identify a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ‘ processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller’, the partners will identify the official authority (legal basis) and record this on relevant records of processing.

The partners, when acting as a Processor, will do so in accordance with an appropriate contract/Data Processing Agreement with the relevant Controller/s.

[Provide details of the legal justification/s for sharing data under this OA and any exemptions that may be applied]

Where consent is relied upon as the legal basis for sharing personal information, explicit and informed consent of the data subject will be obtained.

Data provided by the Parties will not be released to any third party without the permission of the owning organisation.

Partners should not hesitate to share personal data in order to prevent abuse or serious harm, in an emergency or in life-or-death situations. If there are concerns relating to child or adult protection issues, the relevant organisational procedures must be followed.

Data Controller

The responsibility of Data Controller for the data subject to this agreement is held by *[insert appropriate details here]:*

[Explain who is/are the data controller(s) for the data disclosed/exchanged. The responsibility may be shared (data controllers in common) or passed from one organisation to another in line with the flow of data.]

Data quality

Personal data will only be collected using approved collection methods, ensuring the required data is complete and up-to-date. All reasonable steps must be taken to ensure that anyone who has received data is notified of any relevant changes and if any inaccuracies are found the necessary amendments will be made.

Fair processing information

The Parties recognise their responsibilities for being transparent and providing accessible information to individuals about how they will share their personal data.

The Parties will work together to ensure that the individuals concerned know who has, or will have, their data and what it is being used for, or will be used for and provide fair processing (privacy) notices and/or statements.

[Provide details of how individuals will be informed about how their information will be shared If existing privacy statements and fair processing notices do not adequately cover this information sharing arrangement additional measures will need to be taken and should be detailed in this section.]

Operational procedures for sharing

[Describe in this section the detailed procedures to be followed to allow data to be shared, access to systems and any data transfer processes]

Consider the following questions as appropriate:

• Will data be requested or is an automatic data flow being set up?

• If data is being requested what is the procedure to do this?

• What will be the frequency of the data exchange?

• If setting up an automatic data flow how will data be transferred?

• If setting up an automatic data flow what are the security arrangements for the data in transit?

• Who is authorised to view/use the shared data and how?

• What systems are involved in the extraction, transfer and storage of the data?

• Could the data to be shared be transferred using the safe haven arrangements already in place in partner organisations?

• Do any arrangements need to be agreed for the return of data at the end of a contract term or agreed period of service provision?

[Consider if the inclusion of a diagram or flow chart describing the sharing process will aid clarity.]

Confidentiality

The Parties shall at all times comply with the duty of confidentiality towards individuals whose personal data is supplied or made available under this Agreement. For the avoidance of doubt this requirement shall survive termination of this Agreement and employees will continue to be bound by confidentiality after their employment has ended.

Consent

Where they rely on the consent of the Data Subject as the legal basis for sharing personal data, the Parties must ensure that it is freely given, specific, informed and unambiguous for each purpose for which the data is being processed.

[*Insert details of how consent and objections will be handled in this section.]*

Security

The Parties agree to ensure that personal data will be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisation measures

The Parties agree to ensure the reliability of their employees through appropriate training. This should also involve making staff aware of the processes outlined within this sharing agreement.

The information must be stored securely and is the responsibility of all partners to ensure that adequate security arrangements are in place in order to protect the integrity and confidentiality of information shared.

When personal data is processed by a third party, the parties will make sure that it will continue to be protected with adequate security by any other organisations that will have access to it. The party disclosing the information will ensure that the receiving organisation understands the nature and sensitivity of the information and will take all reasonable steps to ensure that those security measures are in place, particularly by ensuring that an agreed set of security standards has been signed up to by all the parties involved

Any loss of data by a recipient partner must be notified to the originating partner at the earliest opportunity.

Training

The Parties agree to train their staff in data protection, security, and legal obligations, dependent on their role, so that they know who has the authority to share personal data under this agreement, and in what circumstances this can take place.

[*Insert details of the training required to support this agreement]*

Data breaches

Any loss of data by a recipient partner must be notified to the originating party at the earliest opportunity. As soon as a Data Controller becomes aware that a personal data breach has occurred, it should without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the controller is able to demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals.

Data Subjects should be notified without undue delay if the personal data breach is likely to result in a high risk to their rights and freedoms, in order to allow them to take the necessary precautions.

Retention and disposal

Personal data disclosed under this agreement will not be held for longer than necessary to fulfil the purpose for which it was collected and will be disposed of securely in accordance with national guidance and each organisation's local information retention and disposal policy.

[If it is possible to agree a set retention period for information shared under this agreement insert the details in this section.]

Data Subject Rights and Freedom of Information

The Parties acknowledge a duty to assist one another in meeting their individual responsibilities in respect of Freedom of Information, Subject Access and other data subject rights (including rights of rectification, erasure, restricting or preventing automated decision making or profiling, data portability) and to provide information subject to this agreement in response to formal requests.

[Insert details of how Subject Access and Freedom of Information requests and other Data Subject rights will be handled in this section.]

Transfer outside of the European Economic Area (EEA)

Personal data supplied under the agreement will not be transferred outside the EEA.

Breach of agreement

Any breach of this agreement should be reported and investigated in line with each Party's incident reporting and management procedure and any relevant statutory guidance.

Complaints

Each Party has a formal procedure by which individuals can direct, their complaints regarding the application of this OA.

Contacts

The primary contact for matters relating to the operation and management of this OA are:

Data Sharing Parties	**Responsible Person**
[Insert organisation details here]	*[Insert job title and contact details here]*
[Insert organisation details here]	*[Insert job title and contact details here]*
Insert rows below as necessary	

Signatories

Signed by

[Enter name and position of person signing]

For and on behalf of

Date

Signed by

[Enter name and position of person signing]

For and on behalf of *[Insert name of the organisation whose employee/s will be granted access to the Council's records and systems]*

Date

Operational Agreement - Appendix 1. Legal framework

The principal laws, regulations and guidance are:

- the Common Law Duty of Confidence
- the Human Rights Act 1998
- the Data Protection Act 1998
- General Data Protection Regulation 2016
- the ICO Data Sharing Code of Practice and Data Sharing Checklists

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

The following legislation requires public authorities to share specific information in certain prescribed circumstances and may provide partner organisations with a legal basis for sharing personal data, including special categories of personal data.

♦ NHS (Venereal Diseases) Regulations 1974

♦ Notifications of Births and Deaths Regulations 1982

♦ Codes of Practice, Mental Health Act 1983, s 1.3 – 1.13 and s 14

♦ Police and Criminal Evidence Act 1984

♦ Public Health Act 1984

♦ Public Health (Infectious Diseases) Regulations 1998

♦ Children's Act 1989 s 47

♦ Abortion Regulations 1991

♦ Finance Act 1994

♦ VAT Act 1994, s 91

♦ Criminal Procedure Investigation Act 1996

♦ Social Security Administration (Fraud) Act 1997

♦ Audit Commission Act 1998

♦ Crime and Disorder Act 1998, s 115

♦ Terrorism Act 2000 s 19

♦ Civil Contingencies Act 2004.

Other legislation concerning sharing personal data:

♦ the Children Act 1989 and 2004

♦ the Crime and Disorder Act 1998

♦ the Health and Social Care Act 2012

♦ the Health and Social Care Act (Quality and Safety) 2015

♦ the Care Act 2014

♦ the Children and Families Act 2014

♦ 'No Secrets', Department of Health 2000

♦ Regulatory Investigatory Powers Act 2000

♦ Police Reform Act 2002

♦ Criminal Justice Act 2003

♦ Civil Contingencies Act 2004

♦ Safeguarding Adults, Association of Directors of Social Services 2005

♦ Housing Act 1989

♦ Police and Justice Act 2006

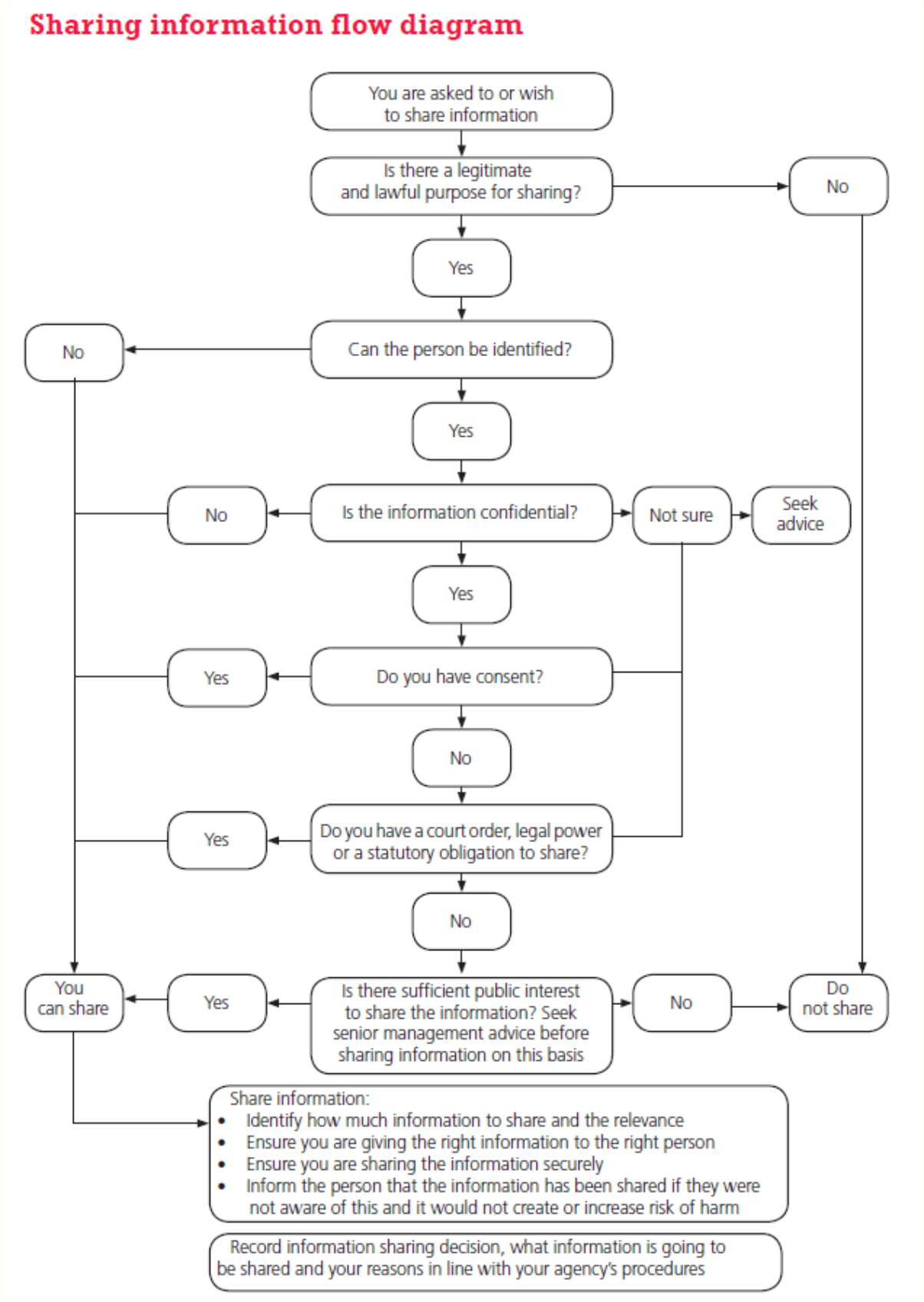
♦ Guidance on the Management of Police Information 2010

♦ Working Together to Safeguard Children 2015 Statutory guidance

♦ Local Government & Public Involvement in Health Act 2007

♦ Children and Young Persons Act 2008.

Appendix 7. Sharing Information Flow Diagram



Appendix 8. Useful links and guidance

Information Commissioner's Office (ICO) (2011) Data sharing code of practice.

https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/

The ICO anonymisation code of practice

https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/

ICO Guide to the General Data Protection Regulation

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

General Data Protection Regulation 2016

https://www.eugdpr.org/article-summaries.html

ICO Guide to the Data Protection Act 2018

https://ico.org.uk/for-organisations/data-protection-act-2018/

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

HM Government 2015 Working together to Safeguard Children

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/592101/Working_Together_to_Safeguard_Children_20170213.pdf

Appendix 9. Glossary

Data Protection Glossary

Anonymised

Turning data into a form which does not identify individuals and where identification is not likely to take place

Consent

Freely given specific and informed indication by which the data subject signifies his or her agreement to personal data relating to him or her being processed. Under the GDPR, consent requires a positive opt-in and pre-ticked boxes or any other method of consent by default should not be used. Consent can be given by a written, electronic, or oral statement.

Explicit consent

A very clear and specific statement of consent for each purpose for which the data is being processed. This must be given for processing special categories of personal data.

Data controller

Person, company or organisation who determines the purpose and manner of the processing of personal data that is the body responsible for the data.

Data processor

Person or organisation which processes personal data on behalf of the data controller. This would include organisations such as IT systems suppliers and people such as market researchers who handle or collect personal data on behalf of the data controller.

Data processing

Obtaining, recording or storing information and carrying out any operation or set of operations upon it, including adaptation, alteration, retrieval, consultation, use, disclosure (sharing), transfer, erasure or destruction.

Data processing agreement

A data processing agreement sets out how a data processor will meet requirements for processing personal data on behalf of the data controller such as where data controller contracts with an IT company to provide data storage services.

Data Protection Impact Assessment (DPIA)

Under the GDPR, data controllers must carry out data protection impact assessments, formerly known as privacy impact assessments. This evaluates the risk to the "rights and freedoms of natural persons" before processing personally identifiable information. The DPIA should include the measures, safeguards and mechanisms that should mitigate the identified risks.

Data subject

Any living person who is the subject of personal data.

Delete/archive

Deletion or removal of data. Data may be deleted on demand or as part of routine removal/record deletions. Data may also be archived which is the process of moving data that is no longer actively used to a separate storage device for long-term retention.

Information sharing agreement

Sets out how partner organisations will meet their respective duties when processing and sharing personal data.

Information asset

A body of information either paper or electronic that is defined and managed as a single unit so it can be understood, shared, protected and used effectively.

Information asset owner (IAOs)

A senior member of staff involved in running the relevant business area whose role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. They are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good.

Information Asset Register

The Information Asset register provides a record of the organisation's information assets (electronic and paper) and details of internal and external data flows. The Information Asset Register enables the organisation to understand and manage the risks to personal data. It should link information assets and systems to data flows, identify where there are data protection impact assessments and information sharing agreements.

Personal data

Information relating to a named or otherwise identifiable individual.

Privacy notice

The detail that appear on consent forms or websites, sometimes called fair processing notices or privacy statements. They are used to inform the person from whom personal data are being collected, how their data will be processed.

Profiling

Use of data processing techniques which consist of creating a profile of an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes, referred to as automated processing.

Recipient

Any person to whom the data are disclosed, including any person to whom they are disclosed in the course of processing the data for the Data Controller. This can be for example, an employee of the data controller, a data processor or employee of the data processor.

Records of processing activity (ROPA)

The details of processing activities that data controllers and data processors are required to record and make available to the ICO on request such as the purposes of processing, categories of personal data, data subjects and recipients, time limits for erasure, description of technical, organisational and security measures.

Special categories of personal data

Personal data containing information relating to the racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life of a data subject, genetic or biometric data that identifies an individual.

System user

Individual who is given access to the information asset or system by the data controller

Appendix 10

Signature sheet

On signing up to the Portsmouth Information Sharing Framework all signatory organisations must demonstrate that by adopting the framework's principles, they will meet or exceed the standards and good practice requirements set out in this document.

	Logo of Organisation	***Name and role of signatory***	***Date***
Jobcentre Plus	Department for Work & Pensions		
Hampshire Constabulary			
Hampshire Fire and Rescue	HAMPSHIRE FIRE AND RESCUE SERVICE		
NHS Portsmouth CCG	NHS Portsmouth Clinical Commissioning Group		
NHS South, Central and West Commissioning Support Unit	NHS South, Central and West Commissioning Support Unit		
Portsmouth City Council Adult Social Care	Portsmouth CITY COUNCIL		
Portsmouth Hospitals NHS Trust	Portsmouth Hospitals NHS NHS Trust		
Solent NHS Trust	Solent NHS NHS Trust		
South Central Ambulance Service NHS Foundation Trust	South Central Ambulance Service NHS NHS Foundation Trust		
University of Portsmouth	UNIVERSITY OF PORTSMOUTH		