Coventry and Warwickshire information sharing strategy

Health and Care Information Sharing Strategy

Information Sharing Advisory Group

Coventry & Warwickshire
Health and Care Information Sharing Strategy

Signatories:

University Hospitals Coventry and Warwickshire
South Warwickshire Foundation Trust
George Elliot Hospital
Coventry and Warwickshire Partnership Trust
Coventry and Rugby Clinical Commissioning Group
South Warwickshire Clinical Commissioning Group
Warwickshire North Clinical Commissioning Group
Warwickshire County Council
Coventry City Council

Contents

Coventry & Warwickshire Health and Care Information Sharing Strategy

Document Control

Document Title:	Coventry & Warwickshire Health and Care Information Sharing Strategy
Description:	An information sharing strategy for use across organisations providing health and social care in Coventry & Warwickshire. It is hoped the scope of this strategy can be expanded to cover all partnership-based information sharing across the sub-region. This document describes our shared commitment to the approach, behaviours and collaboration required to deliver solutions to information sharing requirements. It is intended to provide practical advice to staff needing to undertake information sharing. The Coventry & Warwickshire Information Sharing Protocol, focuses on the information governance aspects
Partners:	University Hospitals Coventry and Warwickshire South Warwickshire Foundation Trust George Elliot Hospital Coventry and Warwickshire Partnership Trust Coventry and Rugby Clinical Commissioning Group South Warwickshire Clinical Commissioning Group Warwickshire North Clinical Commissioning Group Warwickshire County Council Coventry City Council
Author:	Information Governance Working Group
Contact:	andrewmorrall@warwickshire.gov.uk
Owner:	Better Together Programme Board
Version:	1.0
Status:	Approved
Date:	19/01/2016
Protective Marking:	Public
Location	Information Governance Working Group

Version History

Version	Author	Date	Changes
1.0	Spencer Payne	12/05/2016	Approved by the Warwickshire Health and Wellbeing Executive Board at IG Working Group.

1 Introduction

1.1 Information sharing is a vital component of an effective health and social care system. National reviews have highlighted disparity between the principles of information sharing and the application of it by organisations. One key report 'Information Governance: To share or not to share', (published in 2013), highlighted a number of existing practices that organisations must address. This report was led by Dame Fiona Caldicott and seeks to ensure that there can be assurance that patient care is not compromised as a result of a reluctance to share information.

1.2 It is accepted that there is a balance to be had in terms of sharing information. Dame Fiona outlined the following, which summarises the two aspects of the management of information that has to be addressed:

> *'People using health and social care services are entitled to expect that their personal information will remain confidential. They must feel able to discuss sensitive matters with a doctor, nurse or social worker without fear that the information may be improperly disclosed. These services cannot work effectively without trust and trust depends on confidentiality.*
>
> *However, people also expect professionals to share information with other members of the care team, who need to co-operate to provide a seamless, integrated service. So good sharing of information, when sharing is appropriate, is as important as maintaining confidentiality. All organisations providing health or social care services must succeed in both respects if they are not to fail the people that they exist to serve.'*

1.3 To support organisations in making the right decisions, we are guided by the following key laws and guidance:

- Common law duty of confidentiality (see Information Governance Alliance website)
- The Data Protection Act (1998) – The Act provides guidance on how information relating to living people should be processed. It is applicable across the United Kingdom and has a set of eight principles which define the responsibilities for those who store, process or transmit data.
- The Caldicott Principles – These are a set of seven principles which were initially published in 1997 within the Caldicott Report, led by Dame Fiona Caldicott. The report was commissioned to address concerns about how personal information was used within the NHS in England and Wales, as well as identifying whether or not confidentiality was being undermined. Initially there were six principles, the seventh (the duty to share information can be as important as the duty to protect patient confidentiality) was added as a result of the 2013 report again led by Dame Fiona. The Health and Social Care (Safety and Quality) Act 2015 now adds this as a legal duty for sharing health and adult social care data.
- Health & Social Care Information Centre (HSCIC) Confidentiality Rules – In the formal Department of Health response to the 2013 Report, the HSCIC drew up five key rules that NHS organisations should follow, in order to ensure that confidentiality and appropriate sharing of information was maintained.
- HSCIC-hosted Information Governance Toolkit – The IG Toolkit is an online system which allows NHS organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It is submitted annually, using a combination of self-assessment and external validation.

1.4 Further details and definitions on each of the Data Protection Act, Caldicott Principles and Confidentiality Rules can be found at Appendix One.

2 Purpose

2.1 The purpose of this Strategy is to provide a framework by which the sharing of health and care information can be managed effectively and consistently across Coventry & Warwickshire in a secure manner that respects the confidentiality of health and care data.

2.2 This Strategy is based on the good practice template provided by the Information Governance Alliance (IGA).

2.3 At a national and local level there is evidence of a lack of consistency across health, social and private sector organisations in terms of what documentation, assurances and checks need to be undertaken to share information effectively. In order to address some of the concerns that have been raised, the Strategy aims to:

- Provide a consistent approach to information sharing across the sub-region;
- Confirm partners' commitment to establishing information sharing arrangements in a collaborative way, with representatives from commissioning, operational services, information governance, business intelligence and other stakeholders agreeing to work together in a solution-focused way
- Enable appropriate and relevant information flows across organisation boundaries and care settings;
- Support the needs of both direct and indirect care; and
- Continually review the tools available, to ensure that any guidance and documentation remains current and effective.

2.4 These aims will be achieved via the adoption of a joint information sharing business process (presented as a flow chart) and use of national guidance and best practice. This uniform approach, together with an Information Sharing Advisory Group will be used to support the flow of information that is required for care pathways, which assist in ensuring that organisational boundaries are not a barrier to providing the most appropriate and effective service.

2.5 This Strategy is designed to complement the existing Coventry & Warwickshire Information Sharing Protocol. That document focuses on the legal and information governance aspects of information sharing, whereas this Strategy describes the ***collaborative approach and behaviours*** expected of partners in helping establish information sharing.

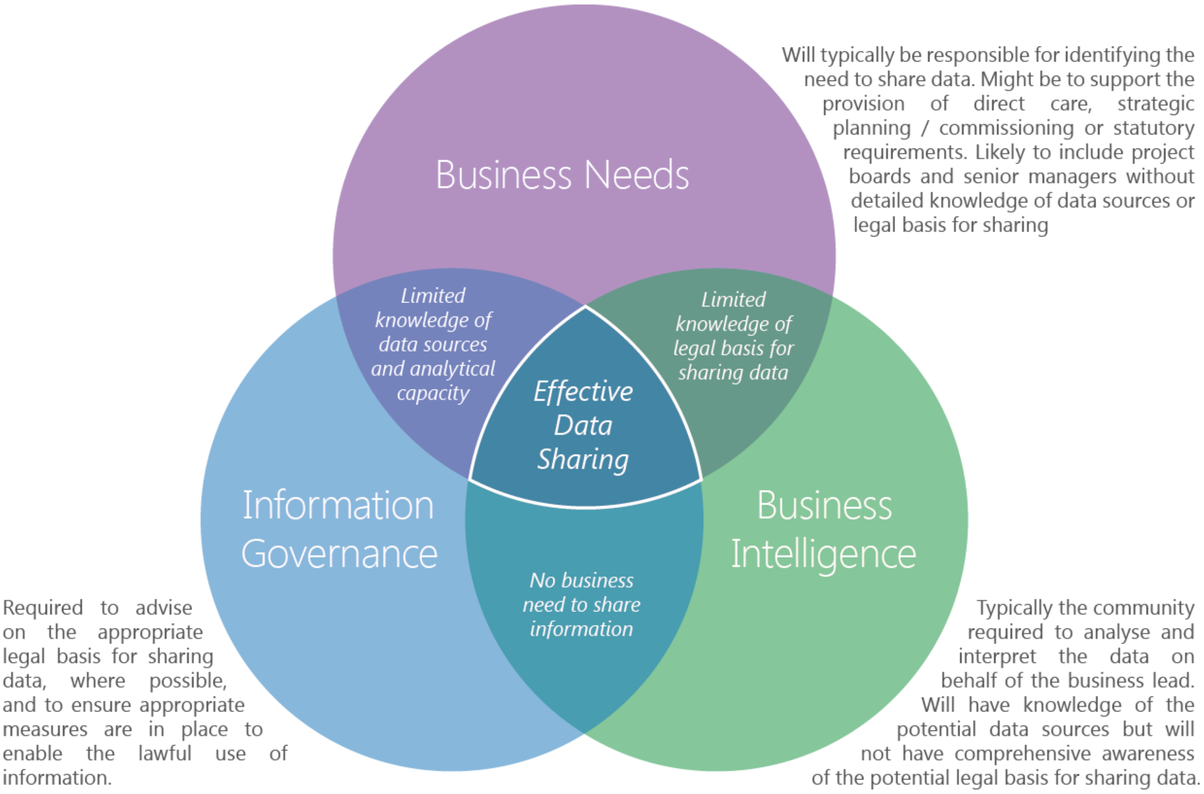
2.6 The IGA has been working with the Department of Health, NHS England, the Health & Social Care Information Centre and a range of local care communities to pull together a package of guidance and materials to support information sharing. The draft framework, published in October 2015, sets out six primary purposes for sharing information, from sharing for direct care to sharing for commissioning. These purposes are listed below and have been incorporated into the flow chart:

- Purpose A **Sharing Information Electronically**: Integrated Digital Care Records
- Purpose B **Care Coordination, Planning and Delivery**: Supporting coordination of care across providers
- Purpose C **Risk Stratification for Case Finding**: Identifying those at risk of an adverse event

- Purpose D **Tracking Outcomes across a Pathway of Care**: Tracking particular cohort groups irrespective of care setting
- Purpose E **Developing Alternative Payment Models including capitated budgets**
- Purpose F **Understanding Current and Future Population Needs**: Strategic and commissioning needs analysis

3 Principles and Approach

3.1 This Strategy commits to the principles of ***collaboration*** (behaviours) and ***fair, lawful information sharing*** (practice). All signatories to this Strategy agree to work together to find constructive solutions to information sharing issues. This involves all stakeholders (the business needs, information governance leads and the business intelligence community) collaborating to agree an approach at the outset of any information sharing process. The diagram below describes why this principle is critical to the Strategy.



Will typically be responsible for identifying the need to share data. Might be to support the provision of direct care, strategic planning / commissioning or statutory requirements. Likely to include project boards and senior managers without detailed knowledge of data sources or legal basis for sharing

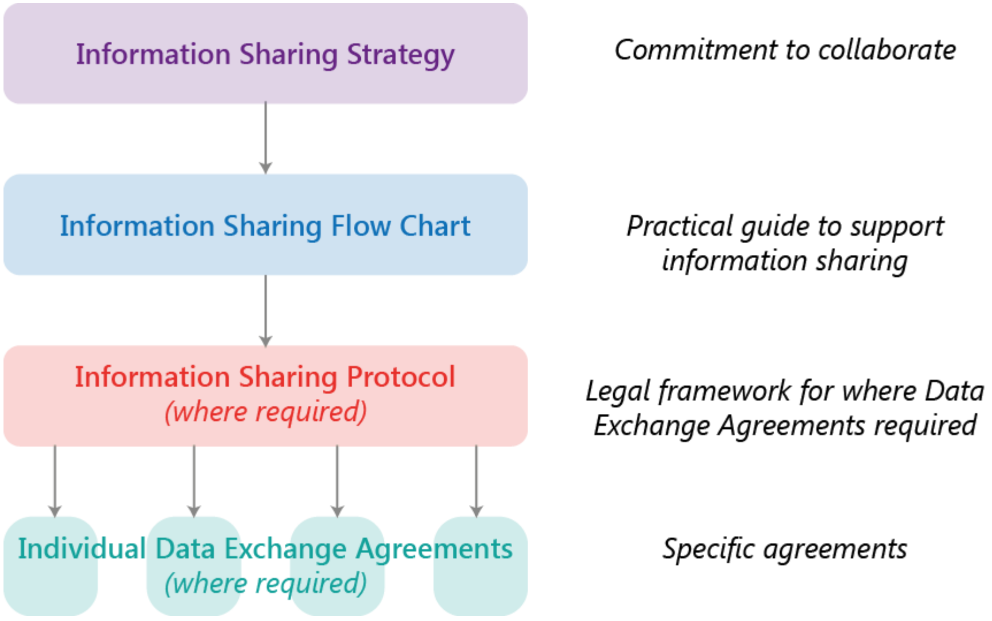
Required to advise on the appropriate legal basis for sharing data, where possible, and to ensure appropriate measures are in place to enable the lawful use of information.

Typically the community required to analyse and interpret the data on behalf of the business lead. Will have knowledge of the potential data sources but will not have comprehensive awareness of the potential legal basis for sharing data.

3.2 This commitment to collaboration is supported by a shared business process, detailed in a flow chart that complements this Strategy. The process advises practitioners (commissioners, project staff etc.) on the appropriate steps to take in order to progress an information sharing requirement. It clearly sets out the responsibilities of the different stakeholders involved in establishing information sharing arrangements and provides clarity on what safeguards and documentation needs to be in place before information sharing can occur.

3.3 The flow chart acts as the practical guide to help translate this Strategy into action. In most cases, and in line with the principles outlined in 3.6, information sharing will be aggregated and depersonalised, and can be completed without needing to refer to the existing Information Sharing Protocol. However, there will be cases where this is required, and the flow chart helps guide practitioners through this process.

3.4 Therefore, this Strategy forms part of a suite of tools that, together, provide the commitment and mechanism to facilitate information sharing across the health and social care sector. The set of documents is illustrated below.



3.5 It is important to understand that this Strategy can be implemented both for sharing information for direct care purposes and for indirect care purposes. The term '**direct care**' means all activities that directly contribute to the diagnosis, care and treatment of the individual. The Caldicott Review defined it as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. '**Indirect care**' purposes are where the benefit of the sharing of information will not directly impact the patient but could bring benefit to the service or to future patients. The Caldicott Review defined this as activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit. HSCIC/IGA/National Data Guardian guidance can be found on their website[1] and will issue further guidance in future.

3.6 This recognises that sharing of information should be done fairly and lawfully and should strike a balance between the specific rights of individuals and the public interest. The following are the principles to be applied whenever personal information is shared or exchanged. The organisations signed up to this strategy are fully committed to ensuring that these standards and principles are adhered to at all times.

- Information about individuals will only be shared when and where it is needed.
- Information will be shared in accordance with statutory duties, underpinned by specific sharing protocols/agreement where appropriate.

---

[1] http://www.hscic.gov.uk/article/3638/Personal-data-access-FAQs

- Information that is provided in confidence will be treated as confidential.
- Information that identifies an individual collected for direct care purposes will only be used for the purposes for which it was collected and shared.
- Individuals will be properly informed about the way their personal information is used and shared and told if it changes.
- Explicit consent to share personal information will be sought wherever appropriate.
- Considerations of confidentiality and privacy will not automatically cease on death.
- The information rights of individuals will be respected and observed.
- Organisations collecting personal information will publish service-specific privacy statements and all sharing agreements.

3.7 The categories of information are defined in Appendix One and the principles are further explained in Appendix Two.

4 Commitments

4.1 Organisations are committed to the implementation of an appropriate level of information governance throughout their organisation, in accordance with recognised standards. They will:

a) Adhere to the principles whenever exchanging personal or personal confidential information, whether with a co-signatory or other agency/organisation

b) Share anonymised/aggregated and pseudonymised (depersonalised) data wherever possible, eliminating the use of personal information except where essential.

c) Ensure that all staff (including temporary employees, contractors and volunteers) are aware of and comply with their responsibilities arising from both these commitments, sharing protocols/agreements and relevant legislation, and receive adequate training in order to do so.

d) Implement their own policies on confidentiality, data protection information security records management and information quality which are appropriate to their organisation and comply with recognised good practice.

e) Establish efficient and effective procedures for:

  - Obtaining informed consent to collect, share and process personal identifiable information wherever reasonably practicable. In the majority of cases, consent to information sharing for direct care is simply **implied** as part of the individual's consent to receive care and treatment as long as they have been provided with fair processing information to explain this and they do not object.
  - Informing individuals when personal information is collected from them about how their information is used, who it will be shared with and their rights to object and obtain access to their personal information held on them.
  - Sharing information without consent when there is a legal reason, recording the reasons for that disclosure and the person responsible for making the decision.
  - Sharing of personal information identified as part of a detailed agreement.
  - Making information-sharing an obligation on staff and allocating senior staff responsibility for making complex disclosure decisions.

- Addressing complaints arising from the misuse or inappropriate disclosure of personal information.
- Enabling access to records of individuals by those individuals on request.
- Amending records where they have been shown to be inaccurate and informing partners.
- Ensuring that personal information is reasonably protected at all times, through the use of appropriate security measures.

f) Work towards reducing duplicated requests for information where several agencies are dealing with a single individual.

g) Develop and work to detailed, specific information sharing protocols/agreements that support identified purposes and comply with the minimum information sharing protocol requirements in Appendix Two.

h) Maintain information that is accurate and up to date and hold information securely according to Information Governance Toolkit standards. Retain and destroy information according to NHS Records Management Code of Practice/Policy and Local Authority retention and disposal schedules, or as required for legal hold or as indicated in the Data Exchange Agreement for the specified information sets.

i) Adopt a suitable procedure for resolving complaints from customers about information-sharing decisions. Issues, incidents and complaints resulting from failures in the specific agreements will be fed into the review processes for the individual protocols.

j) Share information between each other free of charge unless special charging arrangements have been agreed;

k) Ensure that information handling procedures comply with the security classification/protective marking standards of the sharing organisation and that the rights of the sharing organisation are recognised.

l) Ensure their registration as Data Controllers under the Data Protection Act is adequate for the purposes for which they may need to process and share information with one another.

m) Support the principles of equality and diversity within the community and ensure that whenever information is provided to the public it will be supplied in appropriate formats and languages as appropriate.

5 Benefits and Outcomes

5.1 The adoption of uniform documentation and the creation of an Information Sharing Advisory Group to provide guidance and support, if needed, will provide a number of benefits. The virtual information sharing team is not designed to replace the existing IG support within individual organisations, but to provide an overarching and consistent approach to cross-organisational projects and services.

5.2 It is hoped that by having this in place, the following benefits will be achieved:

- Robust and clear processes to enable organisations to share information across boundaries and care settings;
- Development of a culture of collaboration and trust in relation to information sharing;
- Ability to learn from existing information sharing processes;
- Reduction in duplication of information shared;
- Assurance that information is only being used for a specific purpose;
- Availability of a ‘data map’ which will illustrate the flows of information across organisations;
- Evidence of compliance with the relevant statutory requirements; and
- Early collaboration will allow for more timely information sharing, informing key projects and programmes at the right stage.

5.3 The benefits listed above will contribute to improved health and wellbeing outcomes for Coventry & Warwickshire's residents through more effective information sharing.

6 Implementation and Review

6.1 Information sharing was identified as a priority in the Warwickshire Health & Wellbeing Annual Review 2015. To progress that priority, this Strategy has been created through a partnership Information Governance Working Group. It has support from Senior Management within the appropriate organisations and is being championed by the Head of Service for Strategic Commissioning, WCC.

6.2 It is anticipated that the scope of this Strategy will evolve as it is used for different purposes and settings, and it will be reviewed regularly as feedback is received. The aspiration is for the Strategy to expand beyond health and social care and cover all areas of information sharing across the sub-region. Once the approach has become embedded, this review will become less frequent but will be at least annually or when there is a change in guidance or legislation which would impact Information Sharing.

6.3 Organisations make the assumption that in the event of organisational changes the successor bodies will observe the existing strategy and associated agreements until the date of the next review.

6.4 In the first instance the Better Together Programme Board will oversee the implementation of this strategy in Warwickshire and submit the final version and any future amendments to the Health and Wellbeing Board’s Executive Team (HWB Exec Team). Chief Executive level officers represented at the HWB Exec Team will be signatories for the strategy and authorise implementation on behalf of the Health and Wellbeing Board. In Coventry this strategy will be implemented via the Information Sharing Board

6.5 Two Information Sharing Advisory Groups will be established, one for each local authority area, and will be the key delivery mechanism for this strategy. In each area this group will include IG colleagues and business intelligence leads from across all partner agencies, who have led the development of work to date. The intention will be to bring these two groups together to manage issues impacting on the Coventry and Warwickshire footprint wherever necessary and align processes and documentation wherever practicable.

6.6 Where sharing of information is not provided for under legislation, it will be risk based, balancing the possible consequences of sharing against the consequences of not sharing.

6.7 Any issues which cannot be resolved by the group will trigger a request for advice and guidance from the Information Commissioners Office. If the guidance provided is still ambiguous the issue will be escalated in the first instance to the Better Together Programme Board. The escalation of issues will be accompanied by the options for resolution and a detailed risk and impact assessment. Where the risk for sharing information is assessed as low Programme board members and ultimately the Chair will decide upon the preferred option to implement. Where the risk for sharing information is assessed as medium or high programme board will recommend a preferred option to the HWB Exec Team who, in conjunction with Caldicott Guardians or SIROs, decide upon the preferred option to implement.

7 Responsibilities

7.1 The Information Sharing Advisory Group will be responsible for maintaining and updating the documentation following feedback from stakeholders and users. Members of the group will be responsible for ensuring that information about this process is cascaded to their organisations.

7.2 The group will be responsible for the assessment and monitoring of any project/service change where assistance is required. A log will be held of all initiatives that require information sharing support, which will also form the basis for a high level data map. This log will be updated by the Team and will be available for audit and governance purposes.

8 Contacts

8.1 The Information Sharing Advisory Groups will be made up of the following key staff (co-opted when required – these are examples only):

- Andrew Morrall, Corporate Information Manager (Warwickshire County Council)
- Alan Haycock, Compliance & Assurance Manager (NHS Arden and Greater East Midlands Commissioning Support Unit)
- Margaret Russell, Information Governance Manager (South Warwickshire Foundation Trust)
- Harjit Matharu, Head of Information Governance (University Hospitals Coventry and Warwickshire NHS Trust)
- Naomi Wills, Head of Information Governance (Coventry and Warwickshire Partnership Trust)
- Vicky Dumigan, Information Governance & FOI Manager (George Eliot Hospital NHS Trust)

Appendix One - Categories of Information

This Strategy applies to all the categories of information listed below;

Category	Comments
Aggregate/statistical information	Information which does not contain personal information about individuals and is often used for planning service delivery and monitoring performance. It is not subject to the Data Protection Act nor should it be subject to any other restrictions on disclosure. Usually the sort of information that is publicly available or disclosable under the FOI Act, although there may be conditions on its re-use.
Depersonalised/anonymised information	Information which has had any personal information relating to living individuals removed. As this information does not contain personal information about individuals, it is not subject to the Data Protection Act nor should it be subject to any restrictions on disclosure (unless it contains some commercially confidential information- see below).
Pseudonymised information	Information where the personal identifiers have been replaced by an artificially-created identifier so as to conceal the identity of the patient. The links between the artificial and normal identifiers are stored separately and securely, and so the data may still qualify under the Data Protection Act as personal data. Also referred to as linked anonymous data or coded data.
Personal information and sensitive personal information	Information that identifies a living individual and can affect their privacy. Deciding whether information is "personal" and subject to the protection of the Data Protection Act often depends on the context. The Act also defines a particular class of information - "sensitive personal information" - to which greater protection must be given.
Personal Confidential information	Information provided in confidence by another person – this creates a duty of confidence not to disclose further. Confidential information may be personal or non-personal information. Confidential information should not be disclosed without the consent of the person to whom the duty of confidence is owed, unless there are overriding public interest reasons for disclosing it without consent. The fact that a document is marked "confidential" does not automatically mean that it is subject to a duty of confidence. The important characteristic is that it has been provided by a person in the expectation that it will not be further disclosed without the consent of that person, and it is information that has some "quality of confidence" about it (eg it is not trivial, and it is the type of information an emergency court injunction could be obtained to protect). The Government's protective marking scheme gives clear guidance on the circumstances in which "confidential" should be used to mark documents. Health and care organisations are committed to the Caldicott principles when considering whether confidential information should be shared.

Appendix Two - Sharing Personal Information

This Appendix provides more information on the principles established by the Strategy, in the context of information about individuals which is sensitive and personal.

Information about individuals will only be shared when and where it is needed.	Personal information will only be disclosed where necessary and it will always be dealt with in a sensitive and non-discriminatory manner. For all other purposes, information about individual cases will be anonymised. Agencies will exchange statistics and aggregated information wherever possible, reducing the need for individuals to be identified. Where it is agreed that it is necessary for personal information to be shared, information will be shared on a "need to know" basis only. Agreements will be made between agencies defining exactly what information they need for any given purpose, how it will be shared, and who will have access to it.
Information will be shared in accordance with statutory duties.	Organisations will put in place procedures which ensure that the principles of the Data Protection Act 1998 are adhered to. In particular, they recognise the special considerations needed when sharing information defined as "sensitive personal data" in Section 2 of the DPA, that is, information relating to: ● a person's racial or ethnic origin ● his political opinions ● his religious or other similar beliefs ● his trade union membership ● his physical and mental health ● his sexual life ● the commission or alleged commission by him of any offence ● 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. Organisations which have directly obtained this type of information about an individual will usually seek to obtain the explicit consent of that person to disclose that information to another organisation. If consent is not given, because the person is either unable or unwilling to give that consent, or it is not sought due to issues of risk, then the information will only be released if there are statutory grounds for doing so and one of the remaining conditions in Schedule 3 of the DPA can be satisfied. Where consent is required before information can be disclosed, an individual will be made fully aware of what information is to be shared and the purposes for which it will be used.
Information that is provided in confidence will be treated as confidential	Much of the information provided by service users will be considered by them to be confidential in nature. All organisations that are party to this Charter accept this duty of confidentiality and will not disclose such information without the consent of the person concerned, unless there are statutory grounds and an overriding justification for so doing. In responding to information requests from partner agencies, staff in all organisations will respect this responsibility and not seek to override the procedures that each organisation has in place to ensure that information is not disclosed illegally or inappropriately.
Information will only be used for	Organisations will not re-use or abuse information that has been disclosed to them for specific purposes identified in an agreed protocol. Information shared

the purposes for which it was collected and shared.	with another organisation for a specific purpose will only be used for that purpose and not be regarded by that organisation as being generally available for their use. Where further purposes are identified, they must be in the sharing agreement, and steps taken so that the individual concerned is aware.
Individuals will be properly informed about the way their personal information is used and shared.	Individuals in contact with organisations will be properly informed about information that is recorded about them. If an organisation has statutory grounds for restricting an individual's access to information relating to them, then the individual will be told that such information is held and on what grounds it is restricted. Other than this, they will be given every opportunity to gain access to information held about them and to correct any factual errors that may have been made. Similarly, where opinion about them has been recorded and the service user feels this opinion is based in incorrect factual information, they will be given every opportunity to correct the factual error and record their disagreement with the recorded opinion. When disclosing information about an individual, practitioners will clearly identify whether the information being supplied is fact, opinion, or a combination of the two. Wherever professionals request that information supplied by them be kept confidential from the individual concerned, the outcome of this request and the reasons for taking the decision will be recorded. Such decisions will only be taken on statutory grounds. Some agencies may maintain electronic indexes of service users in order to ensure that they are consistently identified across a range of services. These indexes may also be used to ensure that information can be shared securely and enable relevant changes (eg the updating of an address) to be made from a single request or contact. Agencies using these kind of indexes will ensure that the individuals concerned are aware that information they provide will be used to update or create indexed records, and will inform them which other systems the indexes are linked to.
Consent to share information will be sought wherever appropriate.	In the majority of cases, consent to share will be sought from the individual concerned. Where this is not feasible, consent will be sought from a parent or legally registered guardian. Incapacity to consent will be judged on an individual basis, ensuring that young children, individuals subject to mental illnesses, or those who are confused due to age or other conditions, can still exercise their rights to confidentiality whenever they can demonstrate an understanding of them. If a parent or guardian withholds consent and there are no concerns regarding significant harm to the individual, this will be considered to be the same as an individual refusing consent and information will not be shared unless there is a statutory requirement to do so. Whilst the organisations have a commitment to seeking consent before sharing detailed personal information, there will be occasions when the law allows sharing to take place without consent. This will generally take place only where there is a clear and identified risk in not sharing the information, where there is potential harm to an individual, or there is need to take action for the prevention of crime. The decision to share in these cases will be based on appropriate professional judgement and actioned within the requirements of the law. Such decisions must be made at an appropriate level within the agency supplying the information, and the reasons for not

	obtaining consent must be recorded. Each agency must identify who has been given authority to take this kind of decision, and in what circumstances the exercise of that authority is allowed.
Considerations of confidentiality and privacy will not automatically cease on death.	While the requirements of Data Protection Act are specifically related to living individuals, organisations recognise that there may be occasions when information relating to deceased individuals is shared. Where possible, agencies will attempt to identify the wishes of individuals concerning the use of their personal information after death, and to comply with those wishes in line with the duty of confidentiality. Consideration will also be given to any potential impact on the privacy of relatives of deceased individuals when considering how and with whom information about those individuals may be shared. Legal advice will be sought on individual cases.
The information rights of individuals will be respected and observed.	In order to observe the requirements of the Data Protection Act (1998), signatories will also work to ensure that the following principles apply in handling personal information: • where there is a choice as to whether the information can be shared or not, it will be made as easy as possible for an individual to exercise that choice; • information will only be processed without an individual's knowledge where this is necessary for purposes such as national security, public safety, statistical analysis, the protection of the economy, the prevention of crime or disorder, the protection of health or morals, or the protection of the rights and freedoms of others; • only information which is actually needed will be collected and processed; - personal information will only be seen by staff who need it to do their jobs; • any information which is no longer needed will be deleted; • decisions affecting an individual will only be made on the basis of reliable and up to date information; • personal information will be protected from unauthorised or accidental disclosure; • subject to any statutory exemptions, a copy of any information held will normally be provided on request; • any inaccurate or misleading information will be checked and corrected as soon as it is identified; • proper procedures will be in place for dealing promptly with any complaints that are made; and • personal information will be stored securely and for no longer than is necessary. The principles apply to personal information which is held both on computer and in some paper records.
Organisations collecting personal information will publish service-specific privacy statements where appropriate.	In order to comply with the requirements of the Data Protection Act it is good practice to publish privacy statements/fair processing notices which set out who will see the information collected, why it is needed, what will be done with it and how long it will be retained for. It will also state how that personal information is safeguarded, how an individual can check and correct the information that is being held, how to pursue a query or complaint; and where to get more information.