Multi-Agency Overarching Information Sharing Protocol

March 2015– Version 1.0

CONTENTS

1. WELCOME

Partner Agencies have worked together to develop this Multi-Agency Overarching Information Sharing Protocol (the "**Protocol**") to create a positive culture of sharing information and facilitate more effective Data Sharing practices between Partner Agencies, with the aim of improving service delivery.

The Protocol applies to all information being shared by signatory Partner Agencies and it will establish the types of data Partner Agencies will share, how data is handled and the legislation which allows the information to be shared, as well as outlining processes for developing Partner Agency Information Sharing Arrangements.

A list of signatories to the Protocol can be found at Appendix A.

To assist with the understanding of the terms used within the Protocol a Glossary of Terms can be found at Appendix F.

---

2. INTRODUCTION

This Protocol has been developed to ensure that information is being shared lawfully, appropriately and in compliance with best practice. The Protocol aims to establish consistent principles and practices to govern sharing of personal and non-personal information taking place within and between Partner Agencies. The ethos of the Protocol is for Partner Agencies to share information in all situations to improve service delivery and resident outcomes and to support safeguarding, except where it would be unlawful to do so. **Remember, refusing to share any data can be a risk just as much as sharing too much data.**

The Protocol's Effect on Existing Sharing Arrangements between Partner Agencies

This Protocol is considered to be the overarching agreement for the Partner Agencies which sign up to it. However, the Partner Agencies agree and acknowledge that any existing Data Sharing Agreements and/or protocols in place between Partner Agencies will continue, until they are due to be reviewed. If there are any inconsistencies, or conflict with the terms of the Protocol, those existing arrangements should take precedence. If needed, advice should be sought from each Partner Agency's Information Sharing Contact, or Legal Services. On review, any existing Data Sharing Agreements and/or protocols should be updated and amended to ensure they comply with the principles and processes within this Protocol.

The Protocol's Effect on New Sharing Arrangements between Partner Agencies

For new information sharing arrangements between Partner Agencies, employees should refer to the flowchart at Appendix E for guidance as to what action is required to comply with the Protocol, and for details of the applicable processes. If required, a Partner Agency Information Sharing Arrangement should be completed with reference to Appendix J.

This Protocol applies to information shared by Partner Agencies, excluding any information which is already in the public domain. Sharing is not restricted solely to information classified as Personal Data or Sensitive Personal Data by the Data Protection Act 1998. This includes the following information:

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

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

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

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

---

3. AIMS AND OBJECTIVES OF THE PROTOCOL

Partner Agencies and their employees need to feel confident of their obligations when requested, or requesting, to share information. This Protocol aims to ensure compliance and consistency across the county by achieving the following objectives:

a. Creating a legally binding Protocol to govern working practices and create greater transparency, data security and improved services for users;
b. Offering guidance on how to share information lawfully;
c. Increasing understanding of Data Sharing principles and legislation;
d. Developing a Partner Agency Information Sharing Arrangement template (see Appendix J) to make it easier and quicker to formalise local information sharing activities, ensuring risks are managed and providing assurance for staff and service users, whilst ensuring compliance with the overarching Protocol;
e. To protect Partner Agencies from allegations of wrongful use of data
f. To monitor and review information flows.

By becoming a Partner Agency to this Protocol, Partner Agencies are making a commitment to:

a. Apply the "Fair Processing" and "Best Practice" standards that are in the Information Commissioner's Data Sharing Code of Practice and checklists. See: https://ico.org.uk/for-organisations/guide-to-data-protection/data-sharing/
b. Comply with the Data Protection Act and other relevant legislative provisions;
c. Develop Partner Agency Information Sharing Arrangements that comply with the Protocol and clearly and transparently demonstrate the reasons for sharing data and provide assurance on this activity.

---

4. GENERAL PRINCIPLES

This Protocol recognises and promotes recommended good practice and legal requirements to be followed by all Partner Agencies. This Protocol does not alter existing arrangements already in place for urgent sharing, for example, relating to child protection and safeguarding.

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

---

5. DATA SHARING AND THE LAW

Legislation and common law gives information sharing its legal basis. Legislation and common law gives Partner Agencies powers to share information, as well as responsibilities for protecting

information and preventing improper use. The main legal provisions relating to information sharing and the use and protection of personal information are listed and described in further detail in Appendix C: Relevant Legislation.

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

When creating a Partner Agency Information Sharing Arrangement in Appendix J, a lawful basis for the proposed information sharing must be identified and included within the Partner Agency Information Sharing Arrangement.

The Freedom of Information Act 2000 (FOIA)

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

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

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

Access Rights of Data Subjects under the Data Protection Act (DPA)

If a Partner Agency receives a subject access request under section 7 of the DPA and Personal Data is identified as belonging to another Partner Agency or a third party, it will be the responsibility of the receiving Partner Agency to contact the data owner to determine whether the latter wishes to rely on the right to any statutory exemption under the provisions of the DPA. Where the information cannot be provided without disclosing information relating to another individual who can be identified from that information, there is no obligation to comply with the request unless the other individual has consented to the disclosure of the information to the person making the request, or it is reasonable in all the circumstances to comply with the request without the consent of the other individual. In determining whether it is reasonable, regard shall be had, in particular, to:

- any Duty of Confidentiality owed to the other individual;
- any steps taken by the Data Controller with a view to seeking the consent of the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

---

6. INFORMATION COVERED BY THIS PROTOCOL

This Protocol covers the sharing of a range of types of information, including Personal Data, Sensitive Personal Data and Business Sensitive Data (see glossary section for the definitions relating to these terms). **Wherever possible, it is recommended that anonymised, aggregate or pseudonymised data is used to minimise the risk of any data protection**

breaches. If you are in any doubt over whether you can share data and how to go about doing this, you should consult your organisation's Information Sharing Contact, details of which are included in Appendix I.

Anonymised Information

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

However, Partner Agencies should ensure that anonymised data, when combined with other information from the same, or different sources, does not produce any information which can identify individuals, either directly or by summation. Care should also be taken where requests for information are narrow and the data of a small number of individuals is shared. In these circumstances, despite anonymisation, there is still a risk of identification.

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

- **Aggregation:** Aggregation of datasets about individuals into summary tables, so there are no longer rows relating to individuals.

- **Anonymisation:** Removal of identifiers in datasets at the level of individuals, so that there is no means to re-establish the link between the data and the individuals concerned.

- **Psuedonymisation:** Replacement of identifiers with alternative meaningless alphanumeric fields and reduction of potential identifiers to a partial form (e.g. year of birth instead of date of birth, partial post codes). If a set of keys is used to generate the alternative identifiers, then records relating to the same individual can be linked across datasets treated in the same way where research objectives require this.

---

7. ORGANISATIONAL RESPONSIBILITIES

Each Partner Agency is responsible for ensuring that their organisation and security measures protect the information shared under this Protocol.

General responsibilities include:

- Ensuring that the information shared is necessary for the purpose for which it is shared, is shared only with those people who need it, is accurate and up-to-date, is shared in a timely fashion, and is shared, handled and processed securely. The Partner Agency Information Sharing Arrangement will detail these processes in each particular case.

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

- Privacy statements to govern consent for information sharing should be compatible with the aims of this Protocol to ensure that information can be shared within the terms of the consent given and within the reasonable expectations of the individual.

- Partner Agencies should independently or jointly ensure compliance with any Partner Agency Information Sharing Arrangements they are involved in.

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

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

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

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

- Ensure that each Partner Agency Information Sharing Arrangement establishes the specific arrangements for retention and disposal of information for all parties involved, including details of the exact arrangements for the transfer, storage and destruction of data where required.

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

- Decisions about whether to share information or not and the reasoning behind them should be recorded. If you do decide to share information you should record exactly what data was shared, with whom and for what purpose. Specific processes should be recorded in the Partner Agency Information Sharing Arrangement.

- All Partner Agencies agree to publish an approved for publication version of this Protocol on their websites, so the public are aware of the processes in place between signatories for their information to be shared.

- Partner Agencies agree to include details of the Information Sharing Contact at Appendix I.

- Partner Agencies agree to disseminate the training accompanying this Protocol to relevant employees, see Section 14 relating to training for further detail.

Additional Personal & Sensitive Personal Data responsibilities:

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

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

- This Protocol does not intend to give unrestricted access to information. Other Partner Agencies should only be able to access data on a justifiable need to know basis and only relevant employees should be allowed to access the data in order to carry out their duties effectively. Access must be removed when it is no longer necessary.

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

- Information sharing must be compliant with relevant legislation as set out in Appendix C and

with any other conditions Partner Agencies may attach in each agreed Partner Agency Information Sharing Arrangement. The legal basis for sharing must also be recorded in the Partner Agency Information Sharing Arrangement.

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

Non-Personal Data responsibilities:

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

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

---

8. INDIVIDUAL RESPONSIBILITIES

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

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

Every individual should uphold the general principles of confidentiality, and seek advice from their Information Sharing Contact (Appendix I)**.**

Individuals should be made aware that any information breach will be handled in accordance with each Partner Agency's existing disciplinary procedures. Partner Agencies should ensure that their employees are supported by ensuring appropriate employees are provided with the training that accompanies this Protocol.

It is good practice to inform people how their data will be shared and exchanged between Partner Agencies and they should be directed to the published version of this Protocol for information.

---

9. RESTRICTIONS ON USE OF INFORMATION SHARED

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

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

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

For advice on permission to share information you should approach your organisation's Information Sharing Contact (Appendix I).

---

10. CONSENT – APPLIES TO PERSONAL & SENSITIVE PERSONAL DATA ONLY

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

Data Subjects must have the right to withdraw consent at any time; if consent is withdrawn the Partner Agency in question must inform the other Partner Agencies as soon as practicable.

Personal Data can be disclosed in certain circumstances without consent. This depends on certain 'Conditions for Processing' being met as defined in the Data Protection Act. Under the Data Protection Act, in order to disclose Personal Data at least one of the conditions listed in Schedule 2 of the Act must be met. In order to disclose Sensitive Personal Data at least one condition in both Schedules 2 and 3 must be met. Consult the relevant legislation in Appendix C for further detail, and contact your Information Sharing Contact (Appendix I) if you are in doubt.

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

Consent has to be signified by some communication between the Partner Agency and the Data Subject. If the Data Subject does not respond, this cannot necessarily be assumed as implied consent. When using Sensitive Personal Data, explicit consent must be obtained subject to any existing exemptions. In such cases the Data Subject's consent must be clear and cover items such as the specific details of processing, the data to be processed and the purpose.

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

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

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

Again, further detail is provided in Appendix C. The specific details of relating to whether consent will be requested will be recorded in each Partner Agency Information Sharing Arrangement.

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

---

11. SECURITY

Any information shared under this Protocol must be stored securely by the receiving Partner Agency.

It is expected that each Partner Agency has achieved or will aim to work towards information security standards such as ISO 27001, compliance with the NHS Connecting for Health Information Governance Toolkit or will adhere to a similar level of compatible security. Only nominated representatives can access, request information, and make disclosure decisions. Data should be stored securely to prevent unauthorised access and disclosure.

Each Partner Agency agrees to apply appropriate security measures, commensurate with the requirements of principle 7 of the DPA to the data, e.g. make accidental compromise, loss or damage unlikely during storage, handling, use, processing, communication, transmission or transport; deter deliberate compromise or opportunist attack, and promote discretion in order to avoid unauthorised access.

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

a. Ensure that unauthorised staff and other individuals are prevented from gaining access to Personal Data.

b. Ensure visitors are received and supervised at all times in areas where Personal Data is stored.

c. Ensure computer systems containing Personal Data are password protected.

d. Passwords must be treated as private to the individual and must not be disclosed to others.

e. The level of security should depend on the type of data held, but ensure that only those who need to use the data have access.

f. Do not leave your workstation/PC signed on when you are not using it.

g. Lock away disks, tapes or printouts when not in use, as well as USB and other such devices.

h. Ensure all new software has been authorised and disks or storage devices are virus-checked prior to loading onto your PC.

i. Exercise caution in what is sent via email and to whom it is sent; and only transmit Personal Data by email where agreed compatible security arrangements are in place with Partner Agencies (See Appendix G: Government Secure Domains).

j. If information is taken from system/s or network, ensure that appropriate security measures have been taken (e.g. encryption).

k. Ensure the secure disposal of information (electronic and on paper).

l. Check that the intended recipients of faxes, emails and letters containing Personal Data are aware the information is being sent and can ensure security on delivery.

m. Ensure your paper files are stored in secure locations and only accessed by those who need to use them.

n. Do not disclose Personal Data to anyone other than the Data Subject unless you have the Data Subject's consent, or it is a registered disclosure, required by law, or permitted by a Data Protection Act 1998 exemption.

o. Do not leave personal/sensitive personal information on public display in any form. Clear your desk at the end of each day and lock sensitive material away safely.

Each Partner Agency signing this Protocol agrees to adhere to these standards of security. Should additional security arrangements be required, these should be set out in individual Partner Agency Information Sharing Arrangements as required. To determine what security measures are appropriate in any given case, each Partner Agency must consider the type of information and the harm that would arise from a breach of security. In particular, each Partner Agency must consider:

- Where the information is stored;
- The security measures programmed into the relevant equipment;
- The reliability of employees having access to the information.

It is the responsibility of the Partner Agency which discloses Personal Data to make sure that it will continue to be protected by adequate security by any other agencies that access it by including clearly stated requirements in Partner Agency Information Sharing Arrangement. Once the information has been received by the Partner Agency they will have their own legal duties with respect to this information.

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

It is accepted that not all Partner Agencies will have security classification in place, however, it is recommended that signatories to Partner Agency Information Sharing Arrangements: (i) protectively mark the materials they share to indicate the level of sensitivity, and (ii) align the protective marking classification they use with that used by Central Government or similar. Further information is available from the Information Sharing Contacts (Appendix I).

Specific storage and security arrangements, as well as access to data, will all be detailed in the Partner Agency Information Sharing Arrangements, which should be periodically reviewed to ensure that security arrangements are appropriate and effective.

---

12. INFORMATION MANAGEMENT

Data Quality

Information shared should be as complete (but not excessive), accurate and up-to-date as practicable to ensure all Partner Agencies are assured that the information can be used for the purposes for which they require it.

Information discovered to be inaccurate or inadequate for the purpose should be notified to the relevant data owner.

Data Processing

Partner Agencies are expected to ensure that the Personal Data and Sensitive Personal Data they hold is processed in accordance with the Data Protection Act principles (see Appendix C: Relevant Legislation).

Data Retention

Each Partner Agency will apply relevant regulations and timescales to the retention, review and disposal of information (electronic and paper based), only keeping information for as long as is necessary in relation to the purpose it was obtained.

Each Partner Agency must take all reasonable steps to ensure that information is disposed of or destroyed in a way that makes reconstruction unlikely.

The police service is required to retain information in line with the Code of Practice for the Management of Police Information, therefore retention periods for the information shared should be proportionate to the intended purpose and be no more than 6 years

Agencies should also make any Partner Agencies they share information with aware of their rules on data retention and whether these apply to the data being shared.

---

13. TRAINING

An e-learning package has been developed which is offered to Partner Agencies to this Protocol to support implementation. Partner Agencies are encouraged to ensure relevant employees undertake the e-Learning Package which accompanies this Protocol. This training should ideally be completed by employees who will have any responsibility for handling or sharing information, to ensure they can undertake their duties confidently, efficiently and lawfully. This training package will be reviewed on an annual basis alongside the Protocol, as part of the Information Governance Monitoring Group (see Section 15 for further details).

In the alternative, Partner Agencies are encouraged to support implementation of the Protocol by carrying out their own form of training for relevant employees. The training should focus on the principles of the Protocol and the processes involved, in addition to other training that is ordinarily delivered by the Partner Agency. This training should ideally include the following core elements:

- An explanation of the aims and objectives of the Protocol;
- An explanation of the main provisions of the Protocol, including information security and the handling of Personal Data and Sensitive Personal Data;
- An explanation of the process involved in setting up an l Partner Agency Information Sharing Arrangement;
- An explanation of the forms and templates accompanying the Protocol;
- An explanation of the Information Sharing Contacts.

14. REVIEW ARRANGEMENTS

A cross-county Information Governance Monitoring Group will be established, and will meet at least annually; with membership to be comprised of the specialists who act as each organisation's Information Sharing Point of Contact (Appendix I), and who have been delegated to act as such by that organisation's SIRO and/or Caldicott Guardian. The responsibilities of the Information Governance Monitoring Group will be to:

- Review information governance procedures to establish whether they are still effective and working in practice;
- Monitor the effectiveness of the Protocol and associated documents and update the contents when appropriate;
- Share best practice among Partner Agencies and update guidance to reflect this where necessary;
- Build a culture of information sharing between Partner Agencies by proactively communicating the aims of the Protocol;
- Promote and implement education/training practices designed to encourage behaviour change in relation to information sharing;
- Support the development of Partner Agency Information Sharing Arrangements under this Protocol;
- Review and update this Protocol as necessary;
- Review and update the e-learning package accompanying this Protocol as necessary.

Terms of Reference for the Information Governance Monitoring Group will be developed in due course and will be included at Appendix H to this Protocol.

To support smooth implementation of the Protocol an initial early review will take place in May 2015, to be undertaken by the Information Sharing Contact from each Partner Agency. The Information Governance Monitoring Group will be responsible for initiating this process.

Any Partner Agency to this Protocol can request a review at any time where a joint discussion or decision is necessary to address local service developments.

If a significant change takes place which means that the Protocol becomes an unreliable reference point, then it will be updated as needed and a new version which replaces the old will be circulated to all Partner Agencies.

Any Partner Agency can suspend their obligations under the Protocol for 30 days, if they feel that security has been seriously breached or there are concerns over the operation of the Protocol. This should be done in writing and evidence provided to the chairs of the Information Governance Monitoring Group.

Any suspension will be subject to a risk assessment and resolution meeting comprising of all the signatories of the Partner Agencies or their nominated representative. This meeting will take place within 14 days of any suspension.

Any Partner Agency may withdraw from this Protocol. The Partner Agency's signatory to this Protocol must notify the Chairs of the Information Governance Monitoring Group in writing, stating the reason for the withdrawal.

Where a Partner Agency wishes to withdraw due to concerns over the operation of the Protocol, they should first raise their concerns with the Chairs of the Information Governance Monitoring Group, who will initiate an investigation of the Protocol to address the concerns

raised. Where any investigations into concerns do not satisfy the Partner Agency, they may withdraw from this Protocol.

Where more than one Partner Agency wishes to terminate the Protocol, this must be agreed by a majority vote. In such circumstances the Information Governance Monitoring Group will collate the votes for their respective Partner Agencies.

APPENDIX A: SIGNATORIES

Partner Agency Details	Signatory Details	Signature	Date
North Yorkshire County Council County Hall Racecourse Lane Northallerton DL7 8AD	Gary Fielding, Corporate Director Strategic Resources SIRO		
North Yorkshire Police Headquarters Newby Wiske Hall Northallerton DL7 9HA ICO Registration No.: Z4888236	DCC Tim Madgwick SIRO		
City of York Council West Offices Station Rise York YO1 6GA	Ian Floyd Director of Customer and Business Support Services		
North Yorkshire Fire And Rescue Service	Ian Young, Director of Finance and Technical Services (Treasurer) SIRO		
York Teaching Hospitals NHS Trust	Dr Alistair Turnbull, Medical Director and Caldicott Guardian		

APPENDIX B: KEY DOCUMENTS

Document	Purpose	Hyperlink
Multi-Agency Overarching Information Sharing Protocol	The umbrella agreement signed up to by the leaders of participating agencies. Sets out the standards that participating agencies will adhere to when sharing information.	
Partner Agency Information Sharing Arrangement Template	Template for local sharing arrangements under the umbrella of the wider Protocol. Setting the parameters for specific information sharing activities between particular groups of practitioners.	
Contacts	The lead Information Sharing Contacts in each Partner Agency. Available to advise on the application of the Protocol and on information sharing more generally.	
Section 29 Request Form	To be used when requesting information from partners on an ad hoc basis for the prevention and detection of crime, outside of an information sharing arrangement.	
Multi-Agency Overarching Information Sharing Protocol Flowchart	Guidance for information sharing good practice.	
Training Slides	To follow	
Privacy Notice	To follow	
Approved for Publication Version of the Protocol	To follow	

APPENDIX C: RELEVANT LEGISLATION

The ability of Partner Agencies to share information is subject to a number of legal constraints and other considerations such as specific statutory prohibitions on sharing, copyright restrictions or a duty of confidence. If you wish to share information, you must consider whether you have the legal power or ability to do so. This is likely to depend on the nature of the information in question and on which organisations are involved, and which legislation is applicable. The relevant legislation should be identified in the Partner Agency Information Sharing Arrangement, with specific reference to this Appendix C.

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

- **Express obligations** – where a public body is legally obliged to share particular information with a named agency.
- **Express powers** – often designed to permit disclosure of information for certain purposes. Express statutory obligations and powers to share information are often referred to as "gateways".
- **Implied powers** – often legislation regulating public bodies is silent on Data Sharing. In these circumstances, it may be possible to rely upon implied powers to share information derived from express provisions in legislation. Express powers may allow agencies to do other things that are reasonably incidental to those which are expressly permitted.

Whatever the source of an organisation's power to share information, you must check that the power covers the disclosure in question – otherwise you must not share the information unless, in the particular circumstances, there is an overriding public interest in a disclosure taking place. For further information, consult your Information Sharing Contact (hyperlink). Also check whether there is a sector-specific guide addressing the information sharing you intend to undertake, such as the DWP's Guidance for Local Authorities on the use of social security data (2014).

This Appendix is split into two sections:

1. Legislative provisions & guidance relating to sharing and the use and protection of personal information

2. Information sharing powers which may apply to one or more Partner Agencies.

Section 1 – Legislation relating to information sharing

These legislative provisions and guidelines are to be considered when sharing information and when creating a Partner Agency Information Sharing Arrangement. They are not specific information sharing powers (see Section 2 of this Appendix for those) but are relevant and must be given due consideration in each case.

Children Act 2004	Section 10 of the Act places a duty on each children's services authority to make arrangements to promote co-operation between itself and relevant Partner Agencies to improve the well-being of children in their area in relation to: • physical and mental health, and emotional well-being; • protection from harm and neglect; • education, training and recreation; • making a positive contribution to society; and/or • social and economic well-being.
Data Protection Act 1998	8 principles to be complied with: 1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes. 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. 4. Personal data shall be accurate and, where necessary, kept up to date. 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. 6. Personal data shall be processed in accordance with the rights of data subjects under this Act. 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
Gender Recognition Act 2004	Under the Gender Recognition Act 2004 (GRA), individuals who have obtained gender recognition certificates (GRCs) in order to acquire legal status of their transitioned gender are entitled to legal protection from disclosure about their status. It is a criminal offence to disclose this status; i.e. if someone has a gender recognition certificate stating they are a woman, it is a criminal offence to disclose that they used to be a man, except where explicit consent has been obtained from the individual involved or the disclosure is for the purposes of proceedings before a court or tribunal.

Human Rights Act 1998	Article 8 of the Convention gives everyone the right to respect for his private and family life, home and correspondence, and is especially relevant when sharing Personal Data. Article 8 is not an absolute right - public authorities are permitted to interfere with it when the interference is in pursuit of a legitimate aim and it is lawful and proportionate to do so.
Local Government Act 2000	The main power specific to Local Authorities (LAs) is section 2 LGA (2000) – the power of "well-being". This enables LAs to do anything to promote social, economic, or social well- being in their area provided the act is not specifically forbidden by other statute. In addition, S111 LGA (1972) enables LAs to do anything conducive or incidental to the discharge of any of its functions, providing it has specific statutory authority to carry out those main functions in the first place. The above are general powers for LAs but LAs have statutory powers relating to specific activities and these should be referred to as appropriate in any Partner Agency Information Sharing Arrangements.
The Non-Maintained Special Schools Regulations 1999	Require the governing bodies of non-maintained special schools to make arrangements for safeguarding and promoting the health, safety and welfare of pupils at the school as approved by the Secretary of State.
Police Act 1996	Section 30(1) of the PA gives constables all the powers and privileges of a constable throughout England and Wales. Section 30(5) defines these powers as powers under any enactment whenever passed or made. These powers include investigating and detecting crime, apprehension and prosecution of offenders, protection of life and property and maintenance of law and order. Under the Police Reform Act 2002, the Chief Constable can delegate certain powers to police staff.
Safeguarding Vulnerable Groups Act 2006	The Disclosure & Barring Service must maintain the children's barred list and the adult's barred list. Certain roles will require an enhanced DBS check and this will include a check of whether someone is included in the DBS barred list. There are specific rules for carrying out regulated activity with children and/or adults and what checks should be completed with the DBS.

Section 2 – Information Sharing Powers

The following list – which is not exhaustive – highlights legislation with particular relevance to guiding Data Sharing decisions. One or more of these powers must be identified in each Partner Agency Information Sharing Arrangement. There is a specific section relating to the Fire Authority at the end.

The Adoption & Children Act	For further information about the Adoption and Children Act 2002 and Regulations see

2002	www.education.gov.uk/childrenandyoungpeople/families/adoption
Care Act 2014 (from April 2015)	The statutory basis for sharing information that will enable the tracking of patient outcomes across health and care services. The new law means that a person's data can only be shared and analysed when there is a benefit to healthcare, never for other purposes, and that all uses will be scrutinised with full transparency by an independent statutory body Sections 42-47/ Schedule 2 - These sections set out the local authority's responsibility for adult safeguarding for the first time in primary legislation: •responsibility to ensure enquiries into cases of abuse and neglect •establishment of Safeguarding Adults Boards on a statutory footing, • puts Safeguarding Adults Reviews on a statutory footing •information sharing Section 46 repeals section 47 of the 1948 National Assistance Act, which confers a power to remove someone from his or her home in certain circumstances. It is in compatible with human rights legislation and the overall intent of the Act. Section 47 also updates the duty originally set out at section 48 of the National Assistance Act 1948, to protect the property of adults who have been admitted to hospital or residential care, and also re-enacts an offence associated with this duty, found at section 55 of the National Assistance Act 1948. Schedule 2 sets out the membership and funding of Safeguarding Adults Boards (SABs), along with SABs' duties to publish a yearly strategic plan and annual report. Taken as a whole, these provisions set out a new legal framework for adult safeguarding, based on local authorities' existing responsibilities and practice, and current statutory guidance ("No Secrets"). Local authorities should review their current practice, with relevant partners, to determine any specific impacts.
Child Abuse National Protocol	In cases where there is a criminal investigation into alleged child abuse and/or family court proceedings concerning a child the following documents apply to information sharing: • 2013 National Protocol and Good Practice Model – Disclosure of information in cases of alleged child abuse and linked criminal and care directions hearings (Appendix K) • The Local Protocol for North Yorkshire (Appendix L) • Agreed Local Practice for North Yorkshire & York (Appendix M) These documents outline when information in these cases can be shared between North Yorkshire Police, the Local Authorities, and the

	CPS, with specific guidance relating to Family Proceedings material. The Family Procedure Rules also contain provisions for information sharing and they are included below.
Children Act 1989	Sections 17 and 47 of the Children Act 1989 place a duty on local authorities to provide services for children in need and make enquiries about any child in their area who they have reason to believe may be at risk of significant harm. Sections 17 and 47 also enable the local authority to request help from other local authorities, education and housing authorities and NHS bodies and places an obligation on these authorities to co-operate. You may be approached by Children's Services and asked to: - provide information about a child, young person or their family where there are concerns about a child's well-being, or to contribute to an assessment under section 17 or a child protection enquiry; - undertake specific types of assessments as part of a core assessment or to provide a service for a child in need; - provide a report and attend a child protection case conference. The Act does not require information to be shared in breach of confidence, but an authority should not refuse a request without considering the relative risks of sharing information, if necessary without consent, against the potential risk to a child if information is not shared. Section 27 says that the local authority, for assistance in the exercise of its statutory functions (which include the provision of services for children in need and the sharing of information for these purposes) request the help of: • any local authority; • any local education authority; • any health authority; • any person authorised by the Secretary of State. Section 47 of the Children Act 1989 places a duty on local authorities to make enquiries where they have reasonable cause to suspect that a child in their area may be at risk of suffering significant harm. Section 47 states that the authorities listed below must assist a local authority with enquiries of this nature by providing relevant information, unless doing so would cause more harm or be considered unreasonable: • any local authority; • any local education authority; • any housing authority; • any health authority; and/or • any person authorised by the Secretary of State.
Children	The main purpose of the Act is to help young people who have been looked after by a local authority move from care into living

(Leaving Care) Act 2000	independently in as stable a fashion as possible. To do this it amends the Children Act 1989 (c.41) to place a duty on local authorities to assess and meet need. The responsible local authority is to be under a duty to assess and meet the care and support needs of eligible and relevant children and young people and to assist former relevant children, in particular in respect of their employment, education and training. Sharing information with other agencies will enable the local authority to fulfil the statutory duty to provide after care services to young people leaving public care.
Civil Contingencies Act 2004	In emergencies, it may be in the interests of affected vulnerable people for their Personal Data to be shared with emergency responders as defined in the CCA 2004. Sharing personal information may help emergency responders to perform statutory duties. The CCA 2004 1(1) defines an emergency as "an event or situation which threatens serious damage to human welfare and/or the environment or war or terrorism which threatens damage to security". The principles and legislative provisions related to information sharing apply to the planning, response and recovery phases of emergencies.
Common Law (Police)	The Police have a discretionary power (not an obligation) under common law to share information where it is for a policing purpose. For the purposes of this Agreement, police purposes are: • Protecting life and property • Preserving order • Preventing the commission of offences • Bringing offenders to justice, and • Any duty or responsibility of the police arising from common or statute law Any information shared by Police Officers under the common law should only be information that is justified, proportionate and the minimum necessary to achieve the purpose for which it is shared. A record should be kept of any such disclosures, together with details of the rationale behind the decision to share the information.
Common Law Duty of Confidence	The duty of confidence falls within common law as opposed to statutory law and derives from cases considered by the courts. There are three categories of exception: • Where there is a legal compulsion to disclose. • Where there is an overriding duty to the public. • Where the individual to whom the information relates consented. Partner Agencies should consider which of these conditions are the most relevant for the purposes of an agreement. The guidance from the Information Commissioner states that because decisions to disclose 'in the public interest' involve the exercise of judgement it is important that they are taken at an appropriate level and that procedures are developed for taking the decisions. Any Partner Agency Information

	Sharing Arrangement which will impact on the duty of confidence should specify which exception applies.
Crime & Disorder Act 1998 (as amended by the Police and Justice Act 2006)	Section 17 applies to a local authority (as defined by the **Local Government Act 1972**); a joint authority; a police authority; a national park authority; and the Broads Authority. As amended by the **Greater London Authority Act 1999** it applies to the London Fire and Emergency Planning Authority from July 2000 and to all fire and rescue authorities with effect from April 2003, by virtue of an amendment in the **Police Reform Act 2002**. It recognises that these key authorities have responsibility for the provision of a wide and varied range of services to and within the community. In carrying out these functions, section 17 places a duty on them to do all they can to reasonably prevent crime and disorder in their area. The purpose of this section is simple: the level of crime and its impact is influenced by the decisions and activities taken in the day to day business of local bodies and organisations. Section 17 is aimed at giving the vital work of crime and disorder reduction a focus across a wide range of local services that influence and impact upon community safety and putting it at the heart of local decision making. Section 17 is a key consideration for these agencies in their work in crime and disorder reduction partnerships, drug action teams, Youth Offending Teams, children's trusts and local safeguarding children boards. Section 37 sets out that the principal aim of the youth justice system is to prevent offending by children and young people and requires everyone carrying out youth justice functions to have regard to that aim. Section 38(4)(e) requires the provision of reports or other information required by courts in criminal proceedings against children and young persons; Section 39(5) sets out the statutory membership of YOTs reflecting their responsibilities both as a criminal justice agency and a children's service. The membership consists of the following: • at least one probation officer; • at least one police officer; • at least one person nominated by a health authority; • at least one person with experience in education; • at least one person with experience of social work in relation to children. Youth Offending Teams have a statutory duty to coordinate the provision of youth justice services including advising courts, supervising community interventions and sentences, and working with secure establishments in respect of young people serving custodial sentences

	and also in the latter category of a children's service. As Youth Offending Teams are multi-agency teams, Partners will also need to be aware of the need to safeguard and promote the welfare of children that relates to their constituent organisation. Section 115 provides any person with a power (but not an obligation) to disclose information to a "relevant authority" (e.g. police, local and health authorities) and with cooperating bodies (e.g. domestic violence support groups, victim support groups) participating in the formulation and implementation of the local crime and disorder strategy. Information can be shared where the it is 'necessary' or 'expedient' to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder. Section 17 of the Act requires that all local authorities consider crime and disorder reduction while exercising their duties. Sections 5 and 6 of the CDA impose a general duty upon local authorities to formulate and implement a strategy for the reduction of crime and disorder in its area. This ensures that information may be shared for a range of purposes covered by the Act, for example for the functions of the crime and disorder reduction partnerships and Youth Offending Teams, the compilation of reports on parenting orders, anti-social behaviour orders, sex offender orders and drug testing orders.
Criminal Justice Act 2003	Section 325 of this Act details the arrangements for assessing risk posed by different offenders: • The "responsible authority" in relation to any area, means the chief officer of police, the local probation board and the Minister of the Crown exercising functions in relation to prisons, acting jointly. • The responsible authority must establish arrangements for the purpose of assessing and managing the risks posed in that area by: a. relevant sexual and violent offenders; and b. other persons who, by reason of offences committed by them are considered by the responsible authority to be persons who may cause serious harm to the public (this includes children) • In establishing those arrangements, the responsible authority must act in co-operation with the persons identified below. Co-operation may include the exchange of information. The following agencies have a duty to co-operate with these arrangements: a. every youth offending team established for an area b. the Ministers of the Crown, exercising functions in relation to social security, child support, war pensions, employment and training c. every local education authority d. every local housing authority or children's services authority

	e. every registered social landlord which provides or manages residential accommodation f. every health authority or strategic health authority g. every primary care trust or local health board h. every NHS trust i. every person who is designated by the Secretary of State as a provider of electronic monitoring services.
Data Protection Act 1998 Schedules 2 & 3	Disclosure of information amounts to "processing" within the DPA. The first principle, therefore, means that information shall not be disclosed unless Schedule 2, and if information relates to Sensitive Personal Data, Schedule 3 is satisfied. In each Partner Agency Information Sharing Arrangements Form the appropriate Schedule 2 and 3 conditions (or an appropriate exemption) must be specified. The Schedule 2 conditions are: 1. The data subject has given his consent to the processing. 2. The processing is necessary— a) for the performance of a contract to which the data subject is a party, or b) for the taking of steps at the request of the data subject with a view to entering into a contract. 3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract. 4. The processing is necessary in order to protect the vital interests of the data subject. 5. The processing is necessary— (a) for the administration of justice, [(aa) for the exercise of any functions of either House of Parliament,] (b) for the exercise of any functions conferred on any person by or under any enactment, (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or (d) for the exercise of any other functions of a public nature exercised in the public interest by any person. 6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject. 7. The [Secretary of State] may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied. The Schedule 3 conditions are: 1. The data subject has given his explicit consent to the processing of the personal data. 2. (1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed

	by law on the data controller in connection with employment. (2) The [Secretary of State] may by order— (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or (b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
	3. The processing is necessary— (a) in order to protect the vital interests of the data subject or another person, in a case where— (i) consent cannot be given by or on behalf of the data subject, or (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.
	4. The processing— (a) is carried out in the course of its legitimate activities by any body or association which— (i) is not established or conducted for profit, and (ii) exists for political, philosophical religious or trade-union purposes, (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects, (c) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.
	5. The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.
	6. The processing— (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), (b) is necessary for the purpose of obtaining legal advice, or (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.
	7. (1) The processing is necessary— (a) for the administration of justice, [(aa) for the exercise of any functions of either House of Parliament,] (b) for the exercise of any functions conferred on any person by or under an enactment, or (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department. (2) The [Secretary of State] may by order— (a) exclude the application of sub-paragraph (1) in such cases as may be specified, or (b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.
	7A. The processing— (a) is either— (i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or (ii) any other processing by that person or another person of sensitive personal data so disclosed; and (b) is necessary for the purposes of preventing fraud or a particular kind of fraud. (2) In this paragraph “an anti-

	fraud organisation" means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes. 8. The processing is necessary for medical purposes and is undertaken by— (a) a health professional, or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional. (2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services. 9. 1) The processing— (a) is of sensitive personal data consisting of information as to racial or ethnic origin, (b) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and (c) is carried out with appropriate safeguards for the rights and freedoms of data subjects. (2) The [Secretary of State] may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects. 10. The personal data are processed in circumstances specified in an order made by the [Secretary of State] for the purposes of this paragraph
Data Protection Act 1998 (Section 29)	Personal Data processed for the purposes of the prevention or detection of crime or the apprehension or prosecution of offenders are exempt from the non-disclosure provisions of the DPA, where non-disclosure would be likely to prejudice these purposes. This exemption still requires Schedules 2 and 3 to be satisfied. Ad hoc requests to Partner Agencies for disclosure of information under this exemption (and outside of a Partner Agency Information Sharing Arrangement) must be made on the North Yorkshire Section 29 request form at Appendix N.
Data Protection Act 1998 (Section 35)	(1) Personal Data is exempt from the non-disclosure provisions of the DPA where the disclosure is required by or under any enactment, by any rule of law or by the order of a court. (2) Personal Data is exempt from the non-disclosure provisions of the DPA where the disclosure is necessary: a) for the purpose of, or in connection with, any legal proceedings

	(including prospective legal proceedings), or b) for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights. Ad hoc requests to Partner Agencies for disclosure of information under this exemption (and outside of a Partner Agency Information Sharing Arrangement) must be made in writing to the relevant information sharing contact.
Education Act 1996	Section 13 of the Education Act 1996 provides that a local authority shall (so far as their powers enable them to do so) contribute towards the spiritual, moral, mental and physical development of the community, by securing that efficient primary and secondary education is available to meet the needs of the population of the area. Details of the number of children in the local authority's area and an analysis of their needs is required in order to fulfil this duty so there may be an implied power to collect and use information for this purpose. Section 434 (4) of the Act requires local authorities to request schools to provide details of children registered at a school.
Education Act 2002	The section 11 duty of the Children Act 2004 mirrors the duty placed by section 175 of the Education Act 2002 on local authorities and the governing bodies of both maintained schools and further education institutions to make arrangements to carry out their functions with a view to safeguarding and promoting the welfare of children and follow the guidance in Safeguarding Children in Education (DfES 2004). The guidance applies to proprietors of independent schools by virtue of section 157 of the ***Education Act 2002 and the Education (Independent Schools Standards) Regulations 2003***.
Education and Skills Act 2008	Section 17 – Education and Skills Act 2008 – the power for a local authority to share and use information held for purposes of support services or other relevant purposes under the Act. "relevant purpose" means the purpose of, or a purpose connected with, the exercised of any function of the authority, under this part, or under the virtue of sections 68 – 78
The Education (Pupil Information) (England) Regulations 2000	Governs the transfer of information from a maintained school (the old school) when a child moves to a new school. Regulation 10 (3) provides that the head teacher of the pupil's old school, or, if it has been agreed between the head teacher and the local authority, the local authority shall send information (the Common Transfer File and Educational records) to the pupil's new school within 15 school days of the pupil's ceasing to be registered at the old school.
The Education (Pupil	Require all schools to keep admissions and attendance registers, and prescribe the particulars that must be contained in these registers.

Registration) (England) Regulations 2000	They also specify the grounds upon which a pupil's name must be deleted from the admission register and the returns that every school shall make to the local authority. The regulations state that pupils who have been continually unauthorised absent from school for 20 school days must not be deleted from the admission register until both the school and the local authority have failed, after reasonable enquiry, to ascertain where the pupil is. Regulation 12(1) requires every school to inform the local authority about every registered pupil who fails to attend regularly or has been absent without reason for at least 10 school days continuously; Regulation 8 (1) (d) states that pupils can be deleted from the school roll where the school has received written notification from the parent that the pupil is receiving education otherwise than at school. Regulation 12(3) specifies the particular grounds listed under Regulation 8 where schools shall make a return to the local authority as soon as the ground for deletion is met in relation to that pupil, and in any event no later than deleting the pupil's name from the register. This includes pupils deleted under Regulation 8 (1) (d) above.
Education (SEN) Regulations 2001	Regulation 6 provides that when the local education authority are considering making an assessment of a child's special educational needs, they are obliged to send copies of the notice to social services, health authorities and the head teacher of the school (if any) asking for relevant information. Regulation 18 provides that all schools must provide Connexions Services with information regarding all Year 10 children who have a statement of special educational needs.
Family Procedure Rules 2010 – Rule 12.73	The Local Authority may provide to the police, documents or information relating to Family Court proceedings where (a) the police officer to whom disclosure is made is carrying out duties under Section 46 of the Children Act 1989 or serving in a child protection or paedophile unit and (b) disclosure is for the purposes of child protection and not for the purposes of criminal investigation. Where material is disclosed in accordance with this, the police cannot make onward disclosure of any documents or information contained therein for the purposes of the investigation or prosecution without the express permission of the Family Court. For the avoidance of doubt this includes disclosure to the CPS.
Family Procedure Rules 2010 – Rule 12.73(1)(c) & Practice Direction 12G	The text or summary of the whole or part of a judgment given in Family Court proceedings can be shared with the Police/CPS.

Health Act 1999	Section 27 of the Health Act replaces section 22 of the NHS Act 1977. Section 27 states that NHS bodies and local authorities shall cooperate with one another (this allows for practitioners to share information) in order to secure the health and welfare of people.
Housing Act 1985 & 1988	Schedule 2 , para 2 and 14
Housing Act 1996	Sections 135, 152 and 153
Immigration & Asylum Act 1999	Section 20 provides for a range of information sharing for the purposes of the Secretary of State: • to undertake the administration of immigration controls to detect or prevent criminal offences under the Immigration Act; • to undertake the provision of support for asylum seekers and their dependents.
Learning & Skills Act 2000	Section 117 provides for help to a young person to enable them to take part in further education and training. Section 119 enables Connexions services to share information with the Benefits Agency and Jobcentre Plus to support young people to obtain appropriate benefits under the **Social Security Contributions and Benefits Act 1992** and **Social Security Administration Act 1992.**
Local Government Act 2000	Part 1 of the Local Government Act 2000 gives local authorities powers to take any steps which they consider are likely to promote the wellbeing of their area or the inhabitants of it. Section 2 gives local authorities 'a power to do anything which they consider is likely to achieve any one or more of the following objectives': • the promotion or improvement of the economic wellbeing of their area; • the promotion or improvement of the social wellbeing of their area; • the promotion or improvement of the environmental wellbeing of their area. Section 2 (5) makes it clear that a local authority may do anything for the benefit of a person or an area outside their area, if the local authority considers that it is likely to achieve one of the objectives of Section 2(1). Section 3 is clear that local authorities are unable to do anything (including sharing information) for the purposes of the wellbeing of people – including children and young people - where they are restricted or prevented from doing so in the face of any relevant legislation, for example, the Human Rights Act and the Data Protection Act or by the common law Duty of Confidentiality.
National Health	The Act provides for a comprehensive health service to England and Wales to improve the physical and mental health of the population and

Service Act 1977	to prevent diagnose and treat illness. Section 2 provides for sharing information with other NHS professionals and practitioners from other agencies carrying out health service functions that would otherwise be carried out by the NHS.
Mental Capacity Act 2005	• The Mental Capacity Act will apply if there is any doubt that the person concerned has the mental capacity to make specific decisions about sharing information or accepting intervention in relation to their own safety. • The Mental Capacity Act 'Code of practice' (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/224660/Mental_Capacity_Act_code_of_practice.pdf) states that: 'The person who assesses an individual's capacity to make a decision will usually be the person who is directly concerned with the individual at the time the decision needs to be made'. • In most cases a worker should be able to assess whether a person has the mental capacity to make a specific decision – see the **two-stage functional test of capacity**. **The two-stage functional test of capacity** In order to decide whether an individual has the capacity to make a particular decision, you must answer two questions: **Stage 1:** is there an impairment of or disturbance in the functioning of a person's mind or brain? If so, **Stage 2:** is the impairment or disturbance sufficient that the person lacks the capacity to make a particular decision? The Mental Capacity Act states that a person is unable to make their own decision if they cannot do one or more of the following four things: • **understand** information given to them • **retain** that information long enough to be able to make a decision • **weigh up** the information available to make the decision **communicate** their decision – this could be by talking, using sign language or even simple muscle movements such as blinking an eye or squeezing a hand.
The Homelessness Act 2002	This Act relates to local housing authorities and social services authorities in respect of homelessness. The relevant provisions are as follows: S1(6) A social services authority shall take the homelessness strategy for the district of a local housing authority into account in the exercise of their functions in relation to that district. **12 Co-operation in certain cases involving children** After section 213 of the 1996 Act (co-operation between relevant

	housing authorities and bodies) there is inserted— **"213A Co-operation in certain cases involving children** (1) This section applies where a local housing authority have reason to believe that an applicant with whom a person under the age of 18 normally resides, or might reasonably be expected to reside— (a) may be ineligible for assistance; (b) may be homeless and may have become so intentionally; or (c) may be threatened with homelessness intentionally. (2) A local housing authority shall make arrangements for ensuring that, where this section applies— (a) the applicant is invited to consent to the referral of the essential facts of his case to the social services authority for the district of the housing authority (where that is a different authority); and (b) if the applicant has given that consent, the social services authority are made aware of those facts and of the subsequent decision of the housing authority in respect of his case. (3) Where the local housing authority and the social services authority for a district are the same authority (a "unitary authority"), that authority shall make arrangements for ensuring that, where this section applies— (a) the applicant is invited to consent to the referral to the social services department of the essential facts of his case; and (b) if the applicant has given that consent, the social services department is made aware of those facts and of the subsequent decision of the authority in respect of his case. (4) Nothing in subsection (2) or (3) affects any power apart from this section to disclose information relating to the applicant's case to the social services authority or to the social services department (as the case may be) without the consent of the applicant.
The Civil Evidence Act 1995	This Act provides the legal basis for the use of documents and records of any format to be admissible as evidence in civil proceedings. This includes electronic patient records. Statements contained within documents may be admissible even where the original document has been lost and only a copy is available. Documents that form part of a record are also admissible as long as the public authority supplies a signed certificate verifying the authenticity of the document

The Rehabilitation of Offenders Act 1974	Once a caution or conviction has become spent under the 1974 Act, a person does not have to reveal it or admit its existence in most circumstances. Unless an exception applies, then spent cautions and convictions need not be disclosed. An employer cannot refuse to employ someone (or dismiss someone) because he or she has a spent caution or conviction unless an exception applies. The exceptions where you may have to declare spent cautions and convictions are listed in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. An employer should be able to say if an exception applies and, if so, where it can be found on the Exceptions Order.
The Police Reform Act 2002	This Act amends the Crime & Disorder Act 1998, and adds the following: Consultation requirements (1) This section applies to— (a) applications for an anti-social behaviour order; and (b) applications for an order under section 1B. (2) Before making an application to which this section applies, the council for a local government area shall consult the chief officer of police of the police force maintained for the police area within which that local government area lies. (3) Before making an application to which this section applies, a chief officer of police shall consult the council for the local government area in which the person in relation to whom the application is to be made resides or appears to reside. (4) Before making an application to which this section applies, a relevant authority other than a council for a local government area or a chief officer of police shall consult— (a) the council for the local government area in which the person in relation to whom the application is to be made resides or appears to reside; and (b) the chief officer of police of the police force maintained for the police area within which that local government area lies.”
Seriousness Organised Crime and Police Act 2005	s26 provides that any person may disclose information to SOCA if the disclosure is made for the purposes of the exercise by SOCA of any of its functions. SOCA has the functions of preventing and detecting serious organised crime and contributing to the reduction of such crime in other ways. SOCA also has the function of gathering, storing, analysing and disseminating information relevant to the prevention,

	detection, investigation or prosecution of offences or the reduction of crime in other ways. A disclosure under this section does not breach any obligation of confidence owed by the person making the disclosure or any other restriction on the disclosure of information. However, s26 does not authorise a disclosure in contravention of any provisions of the Data Protection Act 1998.
Criminal Justice Act 2003	Under **section 325(3**) of the Criminal Justice Act 2003, health services have a duty to co-operate with the MAPPA responsible authorities in assessing and managing the risk of MAPPA-eligible mentally disordered offenders.
The Police and Justice Act 2006	This Act supplements the crime and disorder provisions as follows: **20 Guidance and regulations regarding crime and disorder matters** (1) The Secretary of State may issue guidance to— (a) local authorities in England, (b) members of those authorities, and (c) crime and disorder committees of those authorities, with regard to the exercise of their functions under [or by virtue of] section 19. (3) The Secretary of State may by regulations make provision supplementing that made by section 19 in relation to local authorities in England. (5) Regulations under subsection (3) or (4) may in particular make provision— (a) as to the co-opting of additional members to serve on the crime and disorder committee of a local authority; (b) as to the frequency with which the power mentioned in section 19(1)(a) is to be exercised; (c) requiring information to be provided to the crime and disorder committee by the responsible authorities and the co-operating persons and bodies; (d) imposing restrictions on the provision of information to the crime and disorder committee by the responsible authorities and the co-operating persons and bodies;

	(e) requiring officers or employees of the responsible authorities and the co-operating persons and bodies to attend before the crime and disorder committee to answer questions; [(6A) In subsection (5)(c) and (d), references to information are, in relation to any crime and disorder committee, to information relating to— (a) the discharge, or decisions made or other action taken in connection with the discharge, by the responsible authorities of their crime and disorder functions; or (b) local crime and disorder matters in relation to which the committee has functions under or by virtue of section 19.]
Crime and Disorder (prescribed Information) Regulations 2007	Relates to the duty to share depersonalised information amongst relevant authorities in a local government area under section 17A of the Crime and Disorder Act 1998. Regulation 2 and the Schedule prescribe the description of information to be shared. Regulation 3 prescribes the interval at which such information must be shared as by the end of each three month period following the three month period to which the information must relate.
Crime and Disorder (Overview and Scrutiny) Regulations 2009	Regulation 5 provides that responsible authorities or co-operating persons or bodies must provide such information as is requested of them by the crime and disorder committee, subject to the provisions in that regulation.
The Criminal Justice and Court Services Act 2000	This Act establishes the Children and Family Court Advisory and Support Service (CAFCASS). 1) In respect of family proceedings in which the welfare of children [other than children ordinarily resident in Wales] is or may be in question, it is a function of the Service to— (a) safeguard and promote the welfare of the children, (b) give advice to any court about any application made to it in such proceedings, (c) make provision for the children to be represented in such proceedings, (d) provide information, advice and other support for the children and their families.
The Caldicott	**a.** Justify the purpose for which the information is needed.

Principles	**b.** Only use personally identifiable information when absolutely necessary. **c.** Use the minimum personal identifiable information possible – if possible use an identifier number rather than a name. **d.** Access to the information should be on a strict need to know basis. **e.** Everyone should be aware of his/her responsibilities to respect client confidentiality. Understand and comply with the law. The most relevant legislation is the Data protection Act 1998, the Police & Criminal Evidence Act 1984 and the Human Rights Act 1998.
Part 2A of the Audit Commission Act 1998	• the Commission may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud, as part of an audit or otherwise; • the Commission may require certain bodies to provide data for data matching exercises. Currently these are all the bodies to which it appoints auditors or which it inspects, other than registered social landlords; • other bodies and persons may participate in its data matching exercises on a voluntary basis where the Commission considers it appropriate. Where they do so, the statute states that there is no breach of confidentiality and generally removes any other restrictions in providing the data to the Commission; • the requirements of the Data Protection Act 1998 continue to apply; • the Commission may disclose the results of data matching exercises where this assists in the prevention and detection of fraud, including disclosure to bodies that have provided the data and to auditors that it appoints; • the Commission may disclose both data provided for data matching and the results of data matching to the Auditor General for Wales, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, for the purposes of preventing and detecting fraud; • wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence; • the Commission may charge a fee to any body participating in a data matching exercise and must set a scale of fees for bodies required to participate; • the Commission must prepare and publish a Code of Practice. All bodies conducting or participating in its data matching exercises, including the Commission itself, must have regard to the Code; and • the Commission may report publicly on its data matching activities.

Section 3 - Fire Authority – Specific Data Sharing Gateways

Fire and Rescue Services Act 2004	**Section 26** provides that a Fire Authority must submit to the Secretary of State any reports and returns and any other information with respect to the Authority's functions which are required by the Secretary of State. S45 provides that an authorised officer may, at any reasonable time, enter premises for the purpose of obtaining information needed for the discharge of a fire authority's functions in relation to extinguishing fires and protecting life and property in the event of fires, rescuing people in the event of road traffic accidents and protecting people from serious harm in the event of road traffic accidents or any other functions conferred on the Authority in relation to other emergencies. It also provides that if there has been a fire in a premise, an authorised officer may enter that premise for the purpose of investigating what caused the fire or why it progressed as it did. However, an authorised officer may not enter premises by force, or demand admission as of right to premises occupied as a private dwelling unless 24 hours' notice in writing has first been given to the occupier of the dwelling. Additionally, an authorised officer may not enter as of right premises in which there has been a fire if the premises are unoccupied but were previously occupied as a private dwelling immediately before the fire unless 24 hours' notice in writing has first been given to the person who was the occupier of the dwelling immediately before the fire. **Section 46** provides that if an authorised officer exercises a power of entry for the purpose of obtaining information needed for the discharge of the fire authority's functions, he may require any person present on the premises to provide him with any facilities, information, documents or records, or other assistance, that he may reasonably request. Similarly, If an authorised officer exercises a power of entry in relation to premises in which there has been a fire, he may, amongst other things; a. inspect and copy any documents or records on the premises or remove them from the premises; b. carry out any inspections, measurements and tests in relation to the premises, or to an article or substance found on the premises, that he considers necessary; c. take samples of an article or substance found on the premises (but not so as to destroy it or damage it unless it is necessary to do so for the purpose of the investigation); d. require a person present on the premises to provide him with any facilities, information, documents or records, or other assistance, that he may reasonably request "Authorised officer" means an employee of a fire authority who is authorised in writing by the authority for these purposes. **Section 6** – in relation to fire safety, provides an implied power share

	information for the purposes of promoting fire safety in its area. **Section 7** – in respect of fire-fighting- provides that (1)A fire and rescue authority must make provision for the purpose of— (a)extinguishing fires in its area, and (b)protecting life and property in the event of fires in its area. (2)In making provision under subsection (1) a fire and rescue authority must in particular— (a)secure the provision of the personnel, services and equipment necessary efficiently to meet all normal requirements; (b)secure the provision of training for personnel; (c)make arrangements for dealing with calls for help and for summoning personnel; (d)make arrangements for obtaining information needed for the purpose mentioned in subsection (1);
Regulatory Reform (Fire Safety) Order 2005	Article 27 – Powers of Inspection: (1) Subject to the provisions of this article, an inspector may do anything necessary for the purpose of carrying out this Order and any regulations made under it into effect and in particular, so far as may be necessary for that purpose, shall have power to do at any reasonable time the following— (a) to enter any premises which he has reason to believe it is necessary for him to enter for the purpose mentioned above and to inspect the whole or part of the premises and anything in them, where such entry and inspection may be effected without the use of force; (b) to make such inquiry as may be necessary for any of the following purposes— (i) to ascertain, as regards any premises, whether the provisions of this Order or any regulations made under it apply or have been complied with; and (ii) to identify the responsible person in relation to the premises; (c) to require the production of, or where the information is recorded in computerised form, the furnishing of extracts from, any records (including plans)— (i) which are required to be kept by virtue of any provision of this Order or regulations made under it; or (ii) which it is necessary for him to see for the purposes of an

	examination or inspection under this article, and to inspect and take copies of, or of any entry in, the records; (d) to require any person having responsibilities in relation to any premises (whether or not the responsible person) to give him such facilities and assistance with respect to any matters or things to which the responsibilities of that person extend as are necessary for the purpose of enabling the inspector to exercise any of the powers conferred on him by this article; (e) to take samples of any articles or substances found in any premises which he has power to enter for the purpose of ascertaining their fire resistance or flammability; and (f) in the case of any article or substance found in any premises which he has power to enter, being an article or substance which appears to him to have caused or to be likely to cause danger to the safety of relevant persons, to cause it to be dismantled or subjected to any process or test (but not so as to damage or destroy it unless this is, in the circumstances, necessary). (2) An inspector must, if so required when visiting any premises in the exercise of powers conferred by this article, produce to the occupier of the premises evidence of his authority. (3) Where an inspector proposes to exercise the power conferred by paragraph (1)(f) he must, if requested by a person who at the time is present in and has responsibilities in relation to those premises, cause anything which is to be done by virtue of that power to be done in the presence of that person. (4) Before exercising the power conferred by paragraph (1)(f) an inspector must consult such persons as appear to him appropriate for the purpose of ascertaining what dangers, if any, there may be in doing anything which he proposes to do under that power.
Localism Act 2011	S9 of the Localism Act amends the Fire and Rescue Services Act 2004 by inserting s5A. This provides that a fire authority may do; a. anything it considers appropriate for the purposes of the carrying-out of any of its functions, b. anything it considers appropriate for purposes incidental to its functions, c. anything it considers appropriate for purposes indirectly incidental to its functions through any number of removes, d. anything it considers to be connected with— i. any of its functions, or ii. anything it may do under paragraph (a), (b) or (c), and e. for a commercial purpose anything which it may do under any of paragraphs (a) to (d) otherwise than for a commercial purpose.

Serious Organised Crime and Police Act 2005	s26 provides that any person may disclose information to SOCA if the disclosure is made for the purposes of the exercise by SOCA of any of its functions. SOCA has the functions of preventing and detecting serious organised crime and contributing to the reduction of such crime in other ways. SOCA also has the function of gathering, storing, analysing and disseminating information relevant to the prevention, detection, investigation or prosecution of offences or the reduction of crime in other ways. A disclosure under this section does not breach any obligation of confidence owed by the person making the disclosure or any other restriction on the disclosure of information. However, s26 does not authorise a disclosure in contravention of any provisions of the Data Protection Act 1998.
Data Protection Act 1998 Schedule 2 & 3	Please refer to section 1 of Appendix C for details
Human Rights Act 1998	Please refer to section 1 of Appendix C for details
Civil Contingencies Act 2004	In emergencies, it may be in the interests of affected vulnerable people for their Personal Data to be shared with emergency responders (i.e.; health service providers, local authorities, police etc. as defined in Schedule 1 of the CCA 2004). Sharing personal information may help emergency responders to perform statutory duties. The CCA 2004 1(1) defines an emergency as “an event or situation which threatens serious damage to human welfare and/or the environment or war or terrorism which threatens damage to security”. The principles and legislative provisions related to information sharing apply to the planning, response and recovery phases of emergencies.
Crime & Disorder Act 1998	S17 applies to a local authority. However, by virtue of Police Reform Act 2002 it also applies to all Fire and Rescue Authorities. S17 recognises that these authorities have responsibility for the provision of a wide and varied range of services to and within the community. In carrying out these functions, s17 places a duty on them to do all they can to reasonably prevent crime and disorder in their area. The purpose of this section is simple: the level of crime and its impact is influenced by the decisions and activities taken in the day to day business of local bodies and organisations. S17 is aimed at giving the vital work of crime and disorder reduction a focus across a wide range of local services that influence and impact upon community safety and putting it at the heart of local decision making. S115 provides any person with a power (but not an obligation) to disclose information to a “relevant authority” (e.g. police, local and health authorities) and with cooperating bodies (e.g. domestic violence support

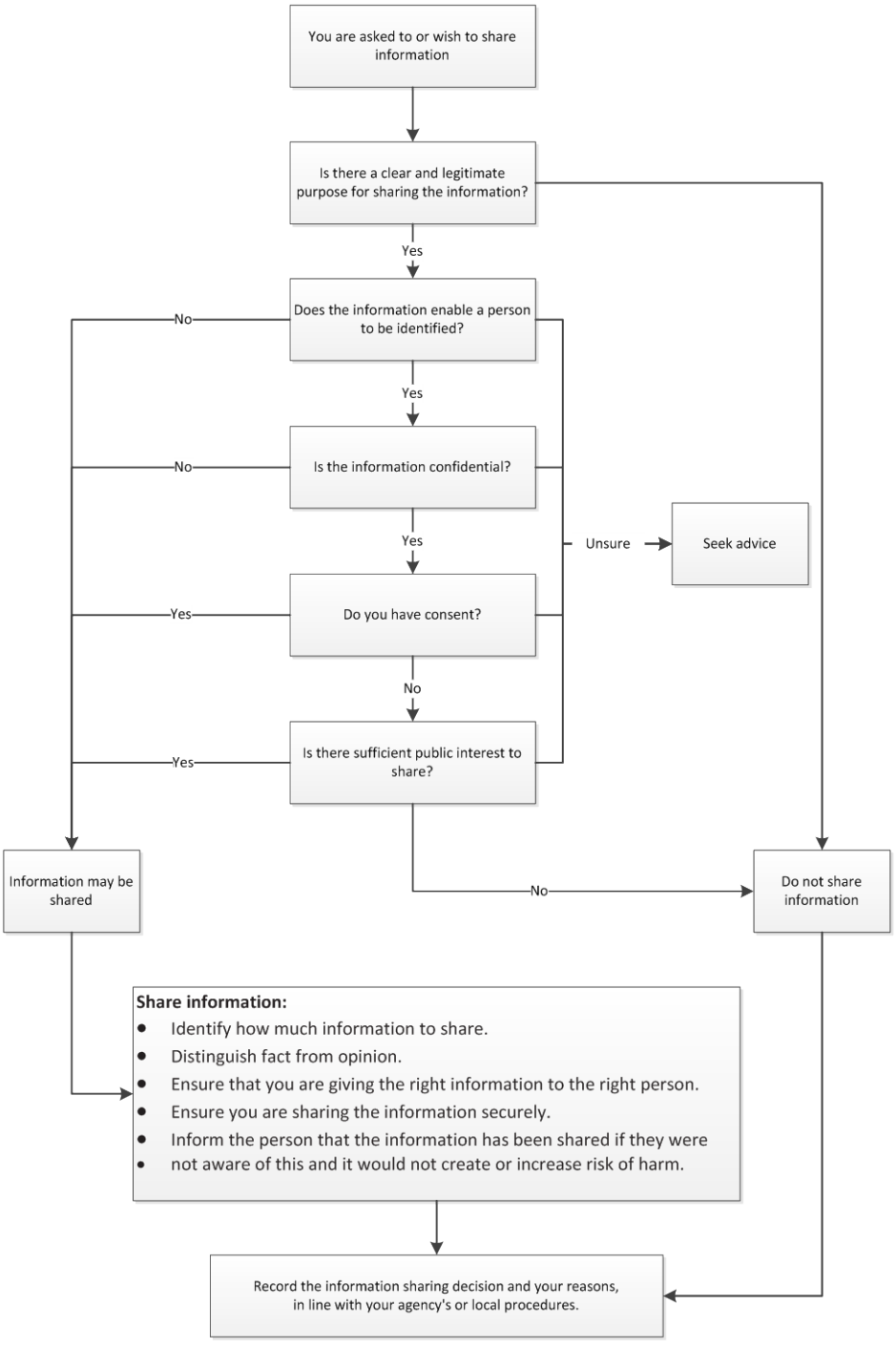
	groups, victim support groups) participating in the formulation and implementation of the local crime and disorder strategy. Information can be shared where the it is 'necessary' or 'expedient' to help implement the provisions of the Act which includes contributing to local strategies to reduce crime and disorder.
Common Law Duty of Confidence	The duty of confidence falls within the common law as opposed to statutory law and derives from cases considered by the courts. There are three categories of exception: • Where there is a legal compulsion to disclose. • Where there is an overriding duty to the public. • Where the individual to whom the information relates consented.

Withholding specific types of Information

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

APPENDIX D - FLOWCHART OF KEY QUESTIONS FOR INFORMATION SHARING

If there are concerns that a child may be at risk of significant harm or an adult may be at risk of serious harm, then follow the relevant procedures without delay.
Seek advice if you are not sure what to do at any stage and ensure that the outcome of the discussion is recorded.



APPENDIX E: PROTOCOL PROCESS FLOWCHART

Is there a need to share personal/sensitive personal identifiable information on an ongoing basis with a Partner Agency?

↓ Yes

↓ Is the partner a signatory to the Protocol?

↓ Yes

Complete a Partner Agency Information Sharing Arrangement in conjunction with the partner organisation. Get it signed by the arrangement owner. Send to your Information Sharing Contact (Appendix I).

↓

Information Sharing Contact shall add the legal basis for sharing and obtains approval from the Information Sharing Approval contact within that organisation.

↓

Once approved, the arrangement will be added to the register held by each organisation's Information Sharing Contact.

↓ No

Complete a Partner Agency Information Sharing Arrangement in accordance with your organisation's existing procedures.

↓ No

No agreement required, make a specific request to the appropriate person within the partner organisation

APPENDIX F: GLOSSARY OF TERMS

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

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

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

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

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

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

Data Sharing – the disclosure of data from one or more agencies to a third party agency(s), or the sharing of data within an agency. Sharing can take the form of systematic, routine data sharing where the same data sets are shared between the same agencies for an established purpose; and exceptional, one off decisions to share data for a range of purposes. Data sharing also includes allowing employees of another partner organisation to access to information, even where a copy of that information is not provided.

Data Sharing Agreements/Protocols – set out a common set of rules to be adopted by the various agencies involved in a Data Sharing operation.

Data Subject – an individual who is the subject of Personal Data.

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

Information Governance Monitoring Group – the cross county group to be set up between the Partner Agencies in accordance with Section 15 of this Protocol

Information Sharing Contact – the lead officer/specialist within each Partner Agency who has been delegated to act as such for the purposes of this Protocol by each agency's SIRO and/or Caldicott Guardian.

Partner– an individual organisation who is a signatory to this Protocol

Partner Agencies – signatories to this Protocol

Partner Agency Information Sharing Arrangement(s) – the individual agreements to be entered into between Partners in conjunction with this Protocol in the form of the template attached as Appendix J.

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

a) from those data, or

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

Privacy Impact Assessment (PIA) – is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure of Personal Data.

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

a) agency, adaptation or alteration of the information,
b) retrieval, consultation or use of the information,
c) disclosure of information by transmission, dissemination or other methods
d) alignment, combination, blocking, erasure or destruction of the information.

Sensitive Personal Data – Personal Data consisting of information as to —

a) the racial or ethnic origin of the Data Subject,
b) his political opinions,
c) his religious beliefs or other beliefs of a similar nature,
d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
e) his physical or mental health or condition,
f) his sexual life,
g) the commission or alleged commission by him of any offence, or
h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

APPENDIX G: GOVERNMENT SECURE DOMAINS

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

x.gsi.gov.uk
gsi.gov.uk
gsx.gov.uk
gse.gov.uk
x.gcsx.gov.uk

.police.uk
.pnn.police.uk
.mod.uk

.cjsm.net
.scn.gov.uk
.nhs.net

APPENDIX H: INFORMATION GOVERNANCE REVIEW GROUP TERMS OF REFERENCE

To follow

APPENDIX I: INFORMATION SHARING CONTACTS

Partner Agency	Name & Role	Contact Details
North Yorkshire County Council	Information Governance Officer, Veritau	information.governance@veritau.co.uk
North Yorkshire Police	Civil Disclosure, Joint Corporate Legal Services	civildisclosure@northyorkshire.pnn.police.uk
City of York Council		
North Yorkshire Fire & Rescue Service	Sarah Dale, Central Administration Manger and Information Governance Officer	Sarah.dale@northyorksfire.gov.uk
York Teaching Hospitals NHS Foundation Trust	Susan Hall, Information Governance Lead	Susan.b.hall@york.nhs.uk 01904 725306

APPENDIX J – PARTNER AGENCY INFORMATION SHARING ARRANGEMENT TEMPLATE

Q:\L & CSD\CivilDisc\
ISA's\COUNTY WIDE

APPENDIX K – 2013 NATIONAL PROTOCOL AND GOOD PRACTICE MODEL

Q:\L & CSD\CivilDisc\
COURT\Info\2013 Dis

APPENDIX L – LOCAL PROTOCOL FOR NORTH YORKSHIRE

Q:\L & CSD\CivilDisc\
COURT\Info\2013 Dis

APPENDIX M – AGREED LOCAL PRACTICE FOR NORTH YORKSHIRE & YORK

Q:\L & CSD\CivilDisc\
COURT\Info\2013 Dis

APPENDIX N – S29 DPA REQUEST FORM

Q:\L & CSD\CivilDisc\
MISC\Templates\App