

SEND Information Sharing Agreement

Children and Young people aged 0-25 with special educational needs or disabilities (SEND)

Version 1.6

Date of Agreement: April 2017



“No serious case review has ever said that ‘too much information was shared between organisations’ though the opposite has all too frequently been the case”



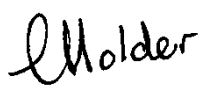



SEND Information Sharing Agreement

Version 1.6

Document History

Version	Date	Author	Released to	Comments
1.1	June 2016	Candy Holder	Sheron Hosking, Adam White, Mazidur Rahman, Mel Davies	Forwarded to CH as track change
1.2	July 2016	Candy Holder	Sheron Hosking, Adam White, Mazidur Rahman, Mel Davies	Version agreed
1.3	September 2016	Candy Holder	Antoinette Carter	Verbal
1.4	September 2016	Candy Holder	Sheron Hosking, Mazidur Rahman, Jo Moses	
1.5	September 2016	Mazidur Rahman	Council Exemptions Panel and Assistant Director of Information Governance at Whittington Health	Minor edits
1.6	February 2017	Mazidur Rahman	Russell Nightingale, Tim Partington, Exemptions Panel	Further amendments as advised by the council's Exemptions Panel

This document requires the following approvals

Agency/Organisation	Post Held	Name	Signature	Date
Islington Council Pupil Services	Head of Pupil Services	Candy Holder		29/04/2017
Islington Council Children's Social Care	Head of Service, Commissioning & Business Support	Jo Moses		01/08/2017
Islington Children's Joint Health Commissioning Team	Head of Children's Health Commissioning	Sheron Hosking		25/05/2017
Whittington Health Integrated Care Organisation	Director, Operations	Russell Nightingale		26/07/2017

Additional signatories in addition to above are included in Appendix A

Copyright Notification

This document is distributed under the Creative Commons Attribution 2.5 license. This means you are free to copy, use and modify all or part of its contents for any purpose as long as you give clear credit for the original creators of the content so used. For more information please see: <http://creativecommons.org/licenses/by/2.5/>

Copyright © London Borough of Islington 2017

CONTENTS

1. Specific purpose for sharing information	5
2. Roles and responsibilities.....	6
3. What information will be shared?	7
4. Legal basis for sharing	8
5. Description of arrangements for sharing	12
Appendix A: Additional Signatories.....	14
Appendix B - The legal basis for information sharing.....	17

1. Specific purpose for sharing information

1.1 This Information Sharing Agreement defines the arrangements for sharing data between partner organisations in the exercise of their duties towards children and young people age 0 to 25 years with special educational needs and disabilities (SEND) and medical needs. It sits beneath Islington Council and Whittington Health Trust's overarching Information Sharing Protocol and builds on 'Working Together to Safeguard Children' (2015) statutory guidance from the Department for Education (DfE).

1.2 The purpose of this agreement is to facilitate information and advice sharing between multi-agency partners in the process of achieving the following aims:

- To improve education, health and emotional wellbeing outcomes for children and young people
- To meet legislative requirements set out in the Children and Families Act 2014
- To improve the quality of provision supported by an holistic assessment of needs and plan
- To ensure effective joint commissioning to address gaps in provision
- To provide a 'tell us once' approach to sharing information and delivery of services. Integrated teams (e.g. co-location of health and social care) and improved joint working (through Lead Professional and 'Team Around the Child' approaches) and workforce development (e.g. multi-agency training) are some ways of achieving this.
- To facilitate requests for High Needs / exceptional funding and allocation and monitoring of any funding agreed
- To ensure continuing health care needs are met in the context of wider social care and education needs
- To support the implementation of the Transforming Care Agenda

1.3 The SEN Code of Practice 2014 makes clear the need for a more joined up approach to working. Paragraph 9.32 states:

"Information sharing is vital to support an effective assessment and planning process which fully identifies needs and outcomes and the education, health and care provision needed by the child or young person. Local authorities with their partners should establish local protocols for the effective sharing of information which addresses confidentiality; consent and security of information. Agencies should work together to agree local protocols for information collection and management so as to inform planning of provision for children and young people with SEN or disabilities at both individual and strategic levels".

1.4 Appropriate information sharing between partner organisations is essential to:

- Support an effective assessment and planning process which fully identifies the education, health and care provision needed by a child or young person. We cannot conduct an assessment or monitor a child or young person's ongoing plan and provision without this
- Support effective decision making in relation to High Needs funding requests and the monitoring of any monies agreed
- Safeguard and promote the well-being of children and young people with SEND in Islington. In line with 'Working Together to Safeguard Children' statutory guidance, early sharing of information is key to providing an effective response to children in need (which includes all children with disability).
- Fulfil statutory duties to jointly commission services for children with disabilities, as set out in the Children and Families Act 2014 and Special Educational Needs and Disability Regulations 2014, services must share information. Effective commissioning must also be underpinned by a Joint Strategic Needs Assessment, which is also a statutory duty under the Health and Social Care Act 2012.

1.5 This agreement will ensure that we are able to meet the statutory requirements of the Children and Families Act 2014 (see Section 4 of this agreement) and share information and advice as part of all statutory processes related to the assessment of children and young people with SEND and any ongoing monitoring, including maintenance of any Education Health and Care (EHC) plans or other relevant plans issued.

1.6 Personal data may also be shared with the Department of Communities and Local Government as part of the Troubled Families Scheme.

Parties to the Agreement

1.7 All partners involved in the continuum of provision that meets the needs of children and young people with SEND and their families are parties to this agreement. This means services across Education, Health and Social Care including:

- Islington Council Pupil Services
- Islington Council Finance Teams
- Islington Council Children's Social Care Teams
- Islington Children's Health Joint Commissioning Team
- Whittington Health Integrated Care Organisation
- Schools including special, secondary, primary, academies
- Out of authority schools, as above attended by Islington residents
- Other educational providers including early years settings, post 16 settings, FE colleges
- Commissioned Services
- Third sector organisations

1.8 Each partner agency will have in place suitable systems and processes that will enable, accurate and timely recording of how information was/was not shared, who requested the information, how it has been recorded and where it can be found.

1.9 Each partner agency remains responsible for the information they store to remain safe and subject to relevant record retention and disposal policies for their organisation, as set out in Section 5 of this agreement. All information technology systems will meet government security requirements.

2. Roles and responsibilities

2.1 The agencies signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of information between their agencies in a manner compliant with their statutory and professional responsibilities.

2.2 As such they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Ensure that where these procedures are complied with, then no restriction will be placed on the sharing of information other than those specified within this agreement.
- Engage in a review of this agreement with partners annually, or as agreed.

2.3 We will require consent from young people or the parents or carers of children with SEND in relation to:-

- Statutory Assessment processes including monitoring of plans where issued, and
- High Needs / exceptional funding processes including assessing requests for funding and the monitoring of any funding agreed
- Continuing Care Assessments
- Transforming Care Community Care and Treatment Reviews (CTRs)

3. What information will be shared?

3.1 The process described in Section 1 above necessitate the sharing of personal and sensitive data and information and advice relating to children, young people and their families and educational providers in relation to:-

- The Statutory Assessment Process and associated decision making systems which may lead to the preparation and issue of an Education, Health and Care (EHC) Plan. This includes the sharing of information and advice with and from contributors to the Statutory Assessment Process. It will ensure Education, Health and Care services have the information they require to inform an EHC plan where this is agreed and the subsequent monitoring and Annual Review of that Plan
- Requests and monitoring information and data relating to High Needs funding processes, such as joint-agency funding of children and young people with complex, multiple and high level needs through the Joint Agency Panel (JAP). This includes information about the child or young person, as well as information specific to the educational setting such as support provided and costs of support

3.2 Personal data that will be shared may include:

Data type	Will this be shared? (Y/N)
Full name	Y
Address	Y
Data of birth	Y
Children's data	Y
Financial data - bank account details, NI numbers	Y
Data about: <ul style="list-style-type: none"> • Ethnicity • Religion • Health • Sexuality • Commission or alleged commission of a crime • Political opinions • Trade union membership 	Y Y Y Y Y N N
Other: <ul style="list-style-type: none"> Personal identifiers e.g. Unique Pupil Number (UPN), NHS number Registered GP Photographs Statutory Plans Safeguarding concerns and other information held that may relate to concerns about neglect / abuse Information to enable audit, quality assurance and self-evaluation / self assurance Protected whereabouts Relevant health information 	Y Y Y Y Y Y Y Y

4. Legal basis for sharing

4.1 Data must be processed lawfully and fairly

Statutory Duties:

The statutory basis for sharing information for this group of children and young people sits within the following:

Children and Families Act 2014, Part 3
Special Educational Needs and Disability Regulations 2014,
Care Act, 2014
Caldicott Principles
NHS Confidentiality Code
Mental Health Act 1983
Mental Capacity Act 2005
Social Care Record Guarantee
Computer Misuse Act 1990
Health and Social Care Act 2012 (Joint Strategic Needs Assessment)

These duties are further exemplified under Appendix B

Common Law duty

The common law duty of confidentiality is derived from case law rather than statute and requires that unless there is a statutory requirement to use information that has been provided in confidence, it should only be used for purposes that the subject has been informed about and consented to. In certain circumstances, this also applies to the deceased. The duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest, for example, to protect others from harm.

4.2 Duty of Confidence and Consent

The starting point in relation to sharing personal and/or confidential information is that practitioners will be open and honest with families and individuals about why, what, how and with whom information will or could be shared.

In line with the Caldicott Review 2013 and Care and Support Statutory Guidance, informed consent should be obtained from the relevant individuals, but if this is not possible and a child is at risk of abuse or neglect, it may be necessary to override the requirement.

Where an individual lacks capacity, staff are expected to make a judgement about whether sharing the information is in their best interests or in the public interest. When considering whether disclosure is in the public interest, for example to prevent or assist in detecting a crime, the rights and interests of the individual must be taken into account. A fair balance between the public interest and the rights of the individual must be ensured.

Any reason for sharing without consent must be fully recorded and the evidence and information on which the decision is based clearly referenced

There is no restriction on sharing depersonalised information, but partner organisations accept that a duty of confidence, contractual or other legal restriction may apply in certain circumstances to some anonymised information.

Partner organisations must take great care when depersonalising information to ensure that an individuals' identity cannot be revealed.

4.3 Fair Processing (Privacy Notice)

The Data Protection Act requires that personal data will be processed fairly and lawfully. In order to achieve this, individuals should be provided with sufficient information in order for them to provide their informed consent for the processing of their data. The law gives organisations some discretion in how they provide fair processing information – ranging from actively communicating it to making it readily available in writing.

The oral or written statement that individuals are given when information about them is collected is often called a 'fair processing' or 'privacy' notice. However, in order to make this notice accessible for the public, it may be helpful to say 'How we use your information'.

All organisations that process personal data should have a 'Privacy Notice' ('How we use your Information') in place that informs individuals about how their personal data will be used by that organisation. This notice should cover:

- The identity of the data controller
- The purpose, or purposes, for which the data are intended to be processed
- Any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair

The Local Authority publishes and keeps under review a Privacy Notice specifically relating to the Education Health and Care Assessment process and partner organisations will all publish a Privacy Notice in their normal manner.

Personal data will be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes detailed in Section 1 of this agreement above, as described in the Fair processing statement

In addition, the information sharing arrangements must satisfy at least one condition in Schedule 2 of the Data Protection Act in relation to personal data. Schedule 2 is satisfied in the case of this agreement by condition 5(b) (the exercise of functions conferred under statute). Where the consent of the individual is received, condition 1 (data subject has given consent to the processing of their data) will apply.

In the case of 'sensitive' information (that is, where it relates to race, ethnic origin, religion or belief system, physical/mental health or sexual life, the commission or alleged commission of any offence, proceedings relating to the offence) at least one condition in Schedule 3 of the Data Protection Act must also be satisfied. It is satisfied in this agreement because the processing is necessary for the exercise of statutory functions (condition 7). Where the consent of the individual is received, condition 1 (data subject has given explicit consent to the processing of their data) applies.

4.4 Legitimate Expectation

The sharing of the information will be done in order to fulfil duties provided by statute law. It can reasonably be assumed that the persons from whom information is obtained will legitimately expect that it will be appropriately shared with any person or agency that will assist in fulfilling the purposes mentioned in Section 1 above.

Consent will have been considered before the individual's information is shared. In cases, where consent has been granted, individuals will have a legitimate expectation of how their data is going to be used and with whom it may be shared and why.

4.5 Personal data

Professionals in partner organisations must handle information on a strictly need-to-know basis for the purposes set out in this agreement. Professionals must be able to justify fully the reasons for their obtaining any particular detail about an individual or any sensitive information.

The Seven Golden Rules for information sharing (DfE, 2015) will be at the centre of working practice for all parties to this agreement, which take full account of the Data Protection Act 1998 and the Human Rights Act - Article 8, the right to respect for private and family life, home and correspondence, as follows:

Information sharing (DfE, 2015) - Seven Golden Rules to Information Sharing

1. Remember that the Data Protection Act is not a barrier to sharing information but provides them with a framework to ensure that personal information about living persons is shared appropriately
2. Are open and honest with the person (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so. Consent should be reviewed on a frequent basis with those who have given it so that it is always current
3. Seek advice if they are in any doubt, without disclosing the identity of the person where possible
4. Share with consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. Information may still be shared without consent if, in their judgement, that lack of consent can be overridden in the public interest. They will base their judgement on the facts of the case
5. Consider safety and well-being, basing their information sharing decisions on considerations of safety and well-being of the person and others who may be affected by their actions
6. Apply the following principles when sharing information, 'necessary, proportionate, relevant, accurate, timely and secure', ensuring that the information shared is necessary for the purpose for which it is being shared, is shared only with those people who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely
7. Keep records of their decisions and the reasons for them – whether it is to share information or not. If the decision is to share the record will indicate what have been shared, with whom and for what purpose.

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.

Secondary use (i.e. sharing of information beyond its original purpose) must not occur without the consent of the data subject (unless there is a legal power or necessity to do so).

Human Rights - right to respect for private and family life

People have the right to withhold personal information and to decline to allow personal information to be shared, although it will also be incumbent on organisations party to this agreement to make clear in such cases the possible consequences in terms of their vital interests, medical needs or ability to fulfil statutory functions, including a responsibility to monitor equality of opportunity. The benefits of effective sharing of information for the purposes set out in this agreement are to the direct benefit of the citizen and so in the public interest.

The promotion of the welfare and wellbeing of children and ensuring they achieve good outcomes is, by virtue of Section 11 of Children Act 2004, a legitimate aim and major responsibility of the signatories to this agreement

Personal data shall be adequate, relevant and not excessive

Any personal data shared will be necessary, proportionate, relevant, accurate, timely and in relation to the purposes set out in Section 1 and the statutory requirements that underpin them as advised by the Data Protection Act 1998 and guidance from the Information Commissioner's Office.

Personal data shall be accurate and, where necessary, kept up to date

Whilst there will be regular sharing of information, much data will be 'historical' in nature. Specifically this means that it exclusively relates to individual actions or events that will have already occurred at the time of sharing. These are not categories of information that will substantially alter or require updating in the future.

It is the responsibility of all staff in each organisation to ensure that information shared is accurate. Where a party to this agreement becomes aware that information shared by them is inaccurate or no longer relevant then they must inform the other parties who will update the records held immediately.

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

Each partner organisation is expected to have a Records Management policy with detailed guidance on retention periods for the full range of education, health and social care records as well as business and corporate records that is in line with the NHS and Social Care Code of Practice and medico-legal requirements.

Transfer of data outside of the European Economic Area

Personal data will not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data.

4.6 Appropriate technical and organisational measures

Partner organisations are expected to have robust information policies in place which apply to all staff, partner organisations, contracted third parties and agents who use facilities and equipment or have access to or custody of client / patient information or other sensitive information.

Information policies should address:

- Code of Conduct for Employees
- ICT Security
- ICT User Management
- ICT Security Incidents
- Third Party Access
- ICT Email
- ICT Physical Security of Information
- ICT Information Risk
- Data transport

5. Description of arrangements for sharing

5.1 Information and advice will be shared via a variety of means between all agencies, including:-

- Secure email
- Secure websites for storage and retrieval of information
- Written and printed hard copy documentation
- Shared via hand delivery or internal and external postal systems (these will be marked confidential and addressed to a specific individual) for example the Head Teacher /Principal/SENCo of an educational provider using Royal Mail Special Delivery.

Movement of Information

5.2 In all cases, the transfer of information will meet the Islington Safeguarding Children Board's requirements and have due regard for the confidentiality and security of the information.

5.3 Staff will be expected to have confirmed the identity of the individual requesting the information prior to sharing any personal information.

5.4 All staff must use their organisations approved secure email system when emailing personal sensitive information.

5.5 Wherever possible, personal/sensitive data shared in hard copy form should be avoided. It is preferable to 'share' data through enabling authorised others to view and update data within partner organisations' record management systems.

5.6 Due care will be taken in sharing paper records and the requesting and disclosing professionals will ensure that any personal or sensitive information is transferred in a secure manner.

Security

5.7 Each organisation must ensure that mechanisms are in place to address the issues of physical security, security awareness and training, security management, systems development, role based security/practitioner access levels, receiving and transfer of data and system specific security policies.

Information Incidents & Breaches of Confidentiality

5.8 Any concerns or complaints received relating to the processing of personal data will be dealt with promptly and in accordance with the internal complaints procedures of that partner organisation and, where appropriate, may be raised with other partner organisation's responsible manager.

5.9 Any breaches will be recorded in accordance to Islington's Security Incident Policy. Each organisation signed up to this agreement needs to notify the partner organisations should any breaches occur.

Indemnity

5.10 Disclosure of personal information without consent must be justifiable on statutory grounds, or meet one or more of the criteria for claiming an exemption under the Data Protection Act. Without such justification, both the agency and the member of staff expose themselves to the risk of prosecution and liability to a compensation order under the Data Protection Act or damages for a breach of the Human Rights Act.

- 5.11** Where a disclosing agency provides information to a requesting agency both parties shall assume that both the request and the disclosure are compliant with the requirements of the Data Protection Act 1998.
- 5.12** If subsequently it is found that the disclosure of information is in contravention of the requirements of the Data Protection Act 1998, the agency that originally breached the requirements of the Data Protection Act 1998, by disclosing information, shall indemnify the other agency against any liability, cost or expense arising directly therefrom, provided that this indemnity shall not apply unless the agency intending to rely on this indemnity notifies the other agency as soon as reasonably practical of any action, claim or demand against itself to which it considers this indemnity may apply, permits that other agency to deal with the action, claim or demand by settlement or otherwise, and renders it all reasonable assistance in doing so.

Staff training

- 5.13** All staff involved in the sharing of information must receive Information Governance training and should undergo refresher courses as directed by their organisation and will comply with all relevant data protection legislations, data transmission, storage, management and disposal policies, regulations and agreements as laid out in their employing organisation.

Compliance

- 5.14** Each organisation must ensure that relevant staff have the necessary level of security clearance.

Storage of Information

- 5.15** Personal and sensitive data will be securely stored by the respective partner organisations, and wherever possible, using access controlled case management systems to restrict the viewing of and access to an individual's records.

Retention & Disposal

- 5.16** Retention and destruction of data will be in line with each partner organisation's records retention policy.
- 5.17** Each organisation should follow its own records retention and disposal process.
- 5.18** All partner organisations should have a confidential and secure process for the destruction of hard copy paper that contains person identifiable information. Prior to the disposal or transfer of ICT equipment and storage devices, signatories to this agreement will have effective processes and procedures in place to ensure, when necessary and appropriate, person identifiable information is deleted to the point where it cannot be reconstructed and that electronic equipment is securely disposed of in line with the Waste Electrical and Electronic Equipment Regulations 2013.

Review & Monitoring of this Agreement

- 5.19** The agreement will be reviewed annually and subject to change dependent on any legislative changes or national guidance.

Appendix A: Additional Signatories

Agency/ Organisation	Post Held	Name	Signature	Date

[illegible]

[illegible]

Appendix B - The legal basis for information sharing

The Children and Families Act 2014 Part 3 is relevant to the need for information sharing, specifically:

Section 26 (joint commissioning arrangements) requires that:

- (1) A local authority in England and its partner commissioning bodies must make arrangements (“joint commissioning arrangements”) about the education, health and care provision to be secured for—
 - (a) children and young people for whom the authority is responsible who have special educational needs, and
 - (b) children and young people in the authority’s area who have a disability.
- (2) In this Part “education, health and care provision” means—
 - (a) special educational provision;
 - (b) health care provision;
 - (c) social care provision.
- (3) Joint commissioning arrangements must include arrangements for considering and agreeing—
 - (a) the education, health and care provision reasonably required by—
 - (i) the learning difficulties and disabilities which result in the children and young people within subsection (1)(a) having special educational needs, and
 - (ii) the disabilities of the children and young people within subsection (1)(b);
 - (b) what education, health and care provision is to be secured;
 - (c) by whom education, health and care provision is to be secured;
 - (d) what advice and information is to be provided about education, health and care provision;
 - (e) by whom, to whom and how such advice and information is to be provided;
 - (f) how complaints about education, health and care provision may be made and are to be dealt with;
 - (g) procedures for ensuring that disputes between the parties to the joint commissioning arrangements are resolved as quickly as possible.
- (4) Joint commissioning arrangements about securing education, health and care provision must in particular include arrangements for—
 - (a) securing EHC needs assessments;
 - (b) securing the education, health and care provision specified in EHC plans;
 - (c) agreeing personal budgets under section 49.
- (5) Joint commissioning arrangements may also include other provision.
- (6) The parties to joint commissioning arrangements must—
 - (a) have regard to them in the exercise of their functions, and
 - (b) keep them under review.
- (7) Section 116B of the Local Government and Public Involvement in Health Act 2007 (duty to have regard to assessment of relevant needs and joint health and wellbeing strategy) applies in relation to functions exercisable under this section.
- (8) A local authority’s “partner commissioning bodies” are—
 - (a) the National Health Service Commissioning Board, to the extent that it is under a duty under section 3B of the National Health Service Act 2006 to arrange for the provision of services or facilities for—

- (i) any children and young people for whom the authority is responsible who have special educational needs, or
 - (ii) any children and young people in the authority's area who have a disability, and
 - (b) each clinical commissioning group that is under a duty under section 3 of that Act to arrange for the provision of services or facilities for any children and young people within paragraph (a).
- (9) Regulations may prescribe circumstances in which a clinical commissioning group that would otherwise be a partner commissioning body of a local authority by virtue of subsection (8)(b) is to be treated as not being a partner commissioning body of the authority.

Section 36 (Assessment of education, health and care needs) requires that:

- (1) A request for a local authority in England to secure an EHC needs assessment for a child or young person may be made to the authority by the child's parent, the young person or a person acting on behalf of a school or post-16 institution.
- (2) An "EHC needs assessment" is an assessment of the educational, health care and social care needs of a child or young person.
- (11) Regulations may make provision about EHC needs assessments, in particular—
 - (a) about requests under subsection (1);
 - (b) imposing time limits in relation to consultation under subsection (4);
 - (c) about giving notice;
 - (d) about expressing views and submitting evidence under subsection (7);
 - (e) about how assessments are to be conducted;
 - (f) about advice to be obtained in connection with an assessment;
 - (g) about combining an EHC needs assessment with other assessments;
 - (h) about the use for the purposes of an EHC needs assessment of information obtained as a result of other assessments;
 - (i) about the use of information obtained as a result of an EHC needs assessment, including the use of that information for the purposes of other assessments;
 - (j) about the provision of information, advice and support in connection with an EHC needs assessment.

Care Act 2014

Paragraphs 14.157-161 of the Care and Support Statutory Guidance underpinning the Care Act 2014 recommend that agencies should draw up a common agreement relating to confidentiality and setting out the principles governing the sharing of information, based on the welfare of the adult or other potentially affected adults. Such agreement should be consistent with the principles set out in the Caldicott Review 2013 (further detail below).

Caldicott Principles

The Caldicott Committee was set up in 1996 by the Chief Medical Officer to review 'all patient-identifiable information which passes from NHS organisations in England to other NHS or non-NHS bodies for purposes other than direct care, medical research or where there is a statutory requirement for information'.

The Committee published six principles, or standards, that are now accepted as the foundation of good practice for handling personal identifiable information: An additional principle "Principle 7" was introduced in September 2013.

Principle 1- Justify the purpose(s)

Every proposed use or transfer of personally-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate Guardian.

Principle 2 - Do not use personally-identifiable information unless it is absolutely necessary

Personally identifiable information items should not be used unless there is no alternative.

Principle 3 - Use the minimum necessary personally-identifiable information

Where use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability.

Principle 4 - Access to information should be on a strict need to know basis

Only those individuals who need access to person identifiable information should have access to it, in order to undertake tasks within their job role, or tasks which they have expressly been given responsibility for.

Principle 5 – Everyone with access to it should be aware of their responsibilities

Action should be taken to ensure that staff handling person identifiable information are aware of their responsibilities and obligations to respect an individual's confidentiality.

Principle 6 – Understand and comply with the law

Every use of person identifiable information should be lawful.

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

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

Caldicott Review 2013

The implications of the Caldicott review for safeguarding adults are:

- Information may only be shared on a 'need to know' basis when it is in the interests of the adult
- Confidentiality must not be confused with secrecy
- Informed consent should be obtained but, if this is not possible and other adults are at risk of abuse or neglect, it may be necessary to override the requirement and
- It is inappropriate for agencies to give assurances of absolute confidentiality in cases where there are concerns about abuse, particularly in those situations when other adults may be at risk.

The NHS Confidentiality Code of Practice

The Confidentiality Code of Practice is to ensure that information given by the patient is treated as confidential information and only to be divulged on a need to know basis. All staff are obliged to adhere to this procedure.

The Mental Health Act 1983

The 1983 Act is largely concerned with the circumstances in which a person with a mental disorder can be detained for treatment for that disorder without his or her consent. It also sets out the processes that must be followed and the safeguards for patients, to ensure that they are not inappropriately detained or treated without their consent. The main purpose of the legislation is to ensure that people with serious mental disorders which threaten their health or safety or the safety of the public can be treated irrespective of their consent where it is necessary to prevent them from harming themselves or others.

Mental Capacity Act 2005

From 1 October 2007 this Act is fully in force in England and Wales. It impacts on all staff working with or caring for adults (16+) who lack mental capacity (or have impaired capacity) to make their own decisions about health, social care and financial matters.

The Act makes clear who has authority to make decisions in certain situations and sets out statutory principles which must guide decision-making.

Doctors have a legal duty to have regard to the Code of Practice in their day to day decisions about the treatment and care of incapacitated patients. So it is important that doctors take steps to familiarise themselves with the legal principles, and the provisions of the Code which are of most relevance to their areas of practice.

Social Care Record Guarantee

The Social Care Record Guarantee for England sets out the rules that govern how service user information is used within both Adults and Children's Social Care Services and what control individuals can have over this. It is based on professional guidelines, best practice and the law and applies to both paper and electronic records. Whilst not a legal document, the Guarantee could be used as the basis for a complaint.

The Social Care Record Guarantee includes information on:

- people's access to their own records,
- how access to an individual's care record will be monitored and policed and what controls are in place to prevent unauthorised access
- options people have to further limit access,
- access in an emergency
- what happens when someone is unable to make decisions for themselves.

Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act would be considered to have committed a disciplinary offence and be dealt with accordingly.

Health and Social Care Act 2012 (Joint Strategic Needs Assessment)

The Joint Strategic Needs Assessment (JSNA) is a statutory obligation and the Health and Social Care Act acknowledges its role in informing the priorities of the Health and Wellbeing Board, outlining the responsibilities of the Local Authority and Clinical Commissioning Group to collaborate in its production.

The ultimate aim of the JSNA is for the information gathered to identify local priorities and support commissioners to commission services and interventions that will achieve better health and wellbeing outcomes.

Within Islington the JSNA is undertaken in partnership by Islington CCG, Islington Council, and a wide range of stakeholders including the Voluntary and Community sector.

The Data Protection Act 1998

Anyone processing personal data must comply with the eight enforceable principles governing the use of personal information. They say that data must be:

1) Fair and lawful

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. Also the processing must adhere to the Fair Processing Code as published by the Information Commissioner's Office.

2) Use for specified purposes

Personal data shall be obtained only for one or more specified purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

3) Adequate, relevant and not excessive

Personal data shall be adequate, relevant and not excessive in relation to the purpose.

4) Accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date.

5) Do not keep longer than necessary

Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

6) Rights given under the Act

Personal data shall be processed in accordance with the rights of the data subjects under the Act.

7) Unauthorised or unlawful processing, loss, destruction and damage

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) Disclosure outside Europe

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.

Personal data covers both facts and opinions about the individual. It also includes Information regarding the intentions of the data controller towards the individual, although in some limited circumstances exemptions will apply. With Processing, the definition is far wider than before. For example, it incorporates the concepts of 'obtaining', 'holding' and 'disclosing'.

Schedule 2 – Conditions relevant for the purposes of the first principle: Processing of any Personal Data

Schedule 2 specifies the conditions relevant for the fair and lawful processing of personal data. Personal data is information which relates to a living individual who can be identified from that data, or from that data and other Information which is, or is likely to come into, the possession of the data controller. This includes opinions about the individual and any indications of the organisation's intentions in respect of that individual. The conditions are:

- The data subject has given consent, or the processing is necessary for:
- The performance of a contract of which the data subject is a party
- The compliance of a legal obligation to which the data controller is subject
- The protection of the vital interests of the data subject
- Administering justice, or for exercising statutory, governmental, or other public functions
- The legitimate interests of the Data Controller

In practice this means Data Controllers must:

- Have legitimate grounds for collecting and using the personal data
- Not use data in ways that have unjustified adverse effects on the individual concerned
- Be transparent about how they intend to use the data, and give individuals appropriate privacy notices when collecting their personal data
- Handle people's personal data only in ways they would reasonably expect; and
- Make sure they do not do anything unlawful with the data.

Schedule 3 – Conditions relevant for the first principle: Processing of Sensitive Personal Data

Sensitive data is 'personal data' that contains information as to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical/mental health, sexual life, or criminal offending.

The conditions are the data subject has given explicit consent, or the processing is necessary:

- To comply with employment law
- For the purpose of, or in connection with legal proceedings
- For the protection of the vital interests (a) of the individual (where their consent cannot be obtained), or (b) another person
- Deliberately made public by the data subject
- Carried out by a not for profit organisation and does not include disclosure to a third party
- In relation to legal proceedings
- For the administration of justice or for exercising statutory of governmental functions
- For medical purposes and undertaken by someone subject to an equivalent duty of confidentiality
- For monitoring equality of opportunity