INFORMATION SHARING POLICY FOR

WEST LONDON PARTNERSHIP SUPPORT UNIT (Connexions and Youth Support Service)

April 2014

Table of Contents

1 OBJECTIVE OF THE POLICY 2

2 KEY TERMS AND DEFINITIONS 3

3 LEGAL FRAMEWORK FOR DATA SHARING 4

3.1 DATA PROTECTION ACT 1998 4
3.2 CHILDREN'S ACT 1989 4
3.3 COMMON LAW OF CONFIDENCE 4
3.4 HUMAN RIGHTS ACT 1998 5
3.5 LEARNING AND SKILLS ACT 2000 5
3.6 CALDICOTT PRINCIPLES 6

4 DATA SUBJECTS 7

5 TYPES OF DATA RETAINED AND WHEN IT MAY BE SHARED 7

5.1 STATISTICAL INFORMATION 7
5.2 BASIC PERSONAL DETAILS 7
5.3 ADDITIONAL PERSONAL INFORMATION 8

6 GENERAL PRINCIPLES OF INFORMATION SHARING 9

6.1 CONFIDENTIALITY AND CONSENT 9
6.2 RELEVANT AGE FOR PROVIDING CONSENT TO INFORMATION SHARING 9
6.3 REFUSAL OF CONSENT 9
6.4 DISCLOSING INFORMATION WITHOUT CONSENT 9
6.5 FURTHER SHARING OF PERSONAL DATA 10
6.6 MINIMAL IDENTIFIABLE INFORMATION 10
6.7 ACCURACY OF THE DATA 10
6.8 SECURITY OF PERSONAL INFORMATION 11
6.9 YOUNG PERSON'S ACCESS TO THEIR INFORMATION 11
6.10 RETENTION OF PERSONAL DATA 12
6.11 RECORDING 12
6.12 THIRD PARTY INFORMATION 12

7 FURTHER OBLIGATIONS 13

7.1 DATA CONTROLLER 13
7.2 LAWFULNESS OF PROCESSING OF DATA 13
7.3 NOTIFICATION UNDER THE DATA PROTECTION ACT 1998 13
7.4 STAFF OBLIGATIONS 13
7.5 COMPLAINTS PROCEDURES 13

8 DECLARATION OF AGREEMENT 14

9 REVIEW OF THE POLICY 15

10 CONTACT FOR THE POLICY 15

Information Sharing Policy for Connexions London West Partnership Support unit and Partnership Agencies

1 OBJECTIVE OF THE POLICY

The Learning and Skills Act 2000 established the Connexions Service to support and encourage young people to continue in, return to and participate effectively in education and training. In September 2002 Connexions London West ("CXLW") was established to deliver services for young people in the West London region (Brent, Ealing, Hammersmith & Fulham, Harrow, Hillingdon and Hounslow). The aim of CXLW is to create an integrated and coherent service to provide information, advice and guidance.

2004 also saw a major structural change in Connexions in West London. Connexions moved to a Confederation Model where each local authority is the lead body for Connexions and Youth Support service in its borough; a development that mirrors national policy in the young people sector and has put West London at the forefront of young people's development. However some functions including Information and Data Management are carried out by the West London Partnership Support Unit jointly funded by all 6 local authorities and based in Ealing. Furthermore since then an additional borough, the London Borough of Barnet has now joined the West London Group.

Furthermore as from April 2014 the London Borough of Barnet has joined the West London group of boroughs to share information through the Core IYSS system having migrated their Integrated Youth Support Service information.

The effective delivery of services to young people within the region depends on partner agencies working together for the benefit of individual young people. Sharing information is an integral part of making the service work for young people. However, it is important that all handling of personal information and any necessary information sharing is done lawfully.

This policy is a statement of the principles and assurances which govern the handling of personal information by the West London Partnership Support Unit to ensure clarity and consistency of practice within the legal framework of:

- Data Protection Act 1998 ("DPA")
- Children's Act 1989
- Common law of confidence
- Human Rights Act 1998
- Learning and Skills Act 2000
- Caldicott Principles
- Other relevant legislation and guidance

Young people have the right to confidentiality and therefore information that identifies individuals should be shared only when there are clear and valid reasons for doing so. This policy sets out the conditions under which information should be shared for the purpose of providing services under Connexions and Youth Support services in West London and LB Barnet.

2 KEY TERMS AND DEFINITIONS

The following terms are used in this document:

Caldicott Guardian - A designated health or social care professional (usually a senior manager) responsible for ensuring that the (Caldicott) principles governing the sharing of patient-identifiable information are adhered to within their organisation.

Data controller - a person who (either jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed. "Person" means a legal person, and includes for example, companies, business, organisations and local and central government.

Data subject - the individual who is the subject of the information;

IYSS – Integrated Youth Support system

PA – Connexions Personal Adviser

Partner Agencies – the providers of services for young people in West London region.

Personal data - 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.

Processing - This means obtaining, recording, or holding (storing) the information or data or carrying out any operation or set of operations on the information or data. The Act makes clear that this can include; organising, adapting, altering, retrieving, consulting, using, disclosing, publishing, aligning, combining, blocking, erasing or destroying the data or the information contained in the data.

Sensitive data - This is personal data revealing an individual's:

- racial or ethnic origin
- political opinions
- religious or other similar beliefs
- trade union membership
- physical or mental health or condition
- sexual life
- (alleged) commission of any offence
- court proceedings for any (alleged) offence

3 LEGAL FRAMEWORK FOR DATA SHARING

Below is a brief summary of the laws relevant to the sharing of personal information.

3.1 Data Protection Act 1998

The Data Protection Act 1998 ("DPA") governs the protection and use of personal information identifying living individuals. The Act gives data subject's rights in relation to the handling of their personal data by data controllers. Data controllers must handle this information in accordance with standards in the Act known as the Data Protection Principles. The principles require personal data to be:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept longer than necessary
6. Processed in accordance with rights of the individual
7. Kept secure
8. Not transferred to countries outside the EU, without adequate protection

The Act is regulated by the Information Commissioner who has a role in promoting good practice and enforcing the Act by investigating breaches (for more information about the Act, see www.informationcommissioner.gov.uk).

3.2 Children's Act 1989

The Act requires that the police and social services are notified of any offence or possible offence against a child or young person.

http://www.hmso.gov.uk/acts/acts1989/Ukpga_19890041_en_1.htm

3.3 Common Law of Confidence

The common law of confidence provides a measure of protection for individuals against unauthorised disclosure of personal information. For an individual to take an action against another person or organisation for breach of the duty of confidence, the individual needs to show that:

1. the information must have the necessary quality of confidence about it;
2. the information was provided in circumstances imposing an obligation of confidence; and
3. that there has been an unauthorised use (or misuse of the information) to the detriment of the party who communicated it.

Some defences to claims of breach of confidence include:

- where the person has consented to the disclosure
- where the person has waived their right to keep the information confidential
- that the information is in the public domain
- that disclosure is in the public interest

Of importance is that, where information has been given to another on the understanding that it will remain confidential, this must be respected unless there is a substantial public interest which overrides this right to confidence.

3.4 Human Rights Act 1998

The Human Rights Act incorporated the European Convention on Human Rights into English law. It is unlawful for a public authority to act in a way that is incompatible with these rights. Of relevance is the right contained in Article 8 which states that:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

However, this right is not absolute. The second part of Article 8 recognises that the right to privacy must be balanced with other public interests. It states that:

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

It is important, however, that any decision to override the right to privacy in the public interest must be proportionate to the aim. This can be explained by the common phrase 'you shouldn't use a hammer to crack a nut'.

3.5 Learning and Skills Act 2000

The Act empowers the following persons and bodies to supply relevant information about young people to Connexions and Youth Support services:

- local authorities
- health authorities
- Learning and Skills Council
- Chief Officer of Police
- Probation Committee
- Youth Offending Teams
- Primary Care Trust

The full text of the Act can be found at: www.hmso.gov.uk/acts/acts2000/20000021.htm

3.6 Caldicott principles

The Caldicott Principles govern the exchange of patient–identifiable information in the health service (NHS Bodies) and between NHS bodies and local authority social services departments.

In some areas they have been adopted as a code of good practice across local authority departments as a condition of data sharing agreements and protocols.

The six principles are:

1. Justify the purpose for which the data is sought
2. Only use patient identifiable information where it is absolutely necessary
3. Use the minimum necessary patient identifiable information
4. Access to patient identifiable information should be on a strict 'need to know' basis.
5. Ensure that everyone with access to patient identifiable information is aware of their responsibilities in relation to it.
6. Users of patient identifiable information must understand and comply with the law.

4 DATA SUBJECTS

This policy concerns the sharing of certain personal information by participating agencies, about the following individuals:

- young people aged between 13 –19 who reside or are in employment, education or training within the following boroughs: Barnet, Brent, Ealing, Hammersmith & Fulham, Harrow, Hillingdon and Hounslow.

- young people up to the age of 25 who have special educational needs of learning difficulties and disabilities, also residing in the above boroughs.

5 TYPES OF DATA RETAINED AND WHEN IT MAY BE SHARED

There are three levels of information retained by West London Partnership Support Unit:

1. Statistical information i.e. information from which the individual can not be identified;
2. Basic personal information e.g. name, address, date of birth, telephone number and/or email address; and
3. Additional personal information

5.1 Statistical Information

Statistical information may be shared within Connexions and Youth Support services in West London, LB Barnet and externally for the following purposes:

To provide management information in order to

- Monitor service delivery
- Monitor outcomes and effectiveness of the service
- Plan service delivery effectively
- Provide partner agencies with information to inform their planning and delivery of provision

The sharing of this aggregate information may be undertaken without seeking consent as individuals cannot be identified from the information and this does not contravene legislation.

5.2 Basic Personal Details

The following basic personal details are retained by West London Partnership Support Unit in order to identify and keep in touch with a young person:

- First name(s) and surname
- Date of birth
- Address including postcode

- Telephone number – at home and mobile (if available)
- E-mail address (if available)

This personal information may need to be shared with other agencies where West London Partnership Support Unit needs to work with these agencies on the young person's behalf in order to provide the full range of services to address the young person's needs. Basic information will be shared immediately with the other agency to ensure that all agencies involved are talking about the same person. Young people must be informed of the sharing of basic information as indicated on the Young Person's Leaflet and recorded on the Connexions and Youth Support services Core IYSS client database (CCIS) and in accordance with relevant legislation.

5.3 Additional Personal Information

Other personal information may be recorded which the young person has shared with his/her Personal Adviser. This may include:

- a record of assessments
- action plans or development plans
- Gender
- Ethnic origin
- Relevant health information
- Special educational needs statement where appropriate
- Information on individual learning difficulties and disabilities (LDD and SEN)
- Current status (in school/college, employed with/without training, unemployed, not known, not available for education/training moved away)
- Name of personal adviser
- Type of contact e.g. interview, telephone, email, group session
- Names of persons in contact with the young person, organisation and contact details. (Subject to written consent where sensitive information may be disclosed relating to a type of organisation, such as if a young person is referred to a Drug Action Team or Youth Offending Team, or is in the care of Social Services.)
- Date of each contact
- support level required
- referral details
- additional support needs (teenage parent, young carer, care leaver, young offender, refugee or asylum seeker, substance misuse etc)

This information is kept so that West London Partnership Support Unit can make sure that it provides appropriate support to the young person. This information may also include "sensitive data" as defined by the Data Protection Act 1998 (see Section 2).

This additional personal information may be shared with other organisations to help the young person progress. This information will only be shared with the young person's consent.

6 GENERAL PRINCIPLES OF INFORMATION SHARING

6.1 Confidentiality and consent

Nationally it has been stated that, as a fundamental principle, Connexions and Youth Support services offers a confidential service to young people. This means that information is only disclosed with the young person's consent or where there are legal requirements to do so.

Consent is a very important element of developing trust in working relationships with young people. The policy of West London Partnership Support Unit is to ensure that the sharing of additional personal data (see Section 5.3) is only done with the young person's informed consent.

6.2 Relevant age for providing consent to information sharing

It is the view of the Information Commissioner (who is responsible for upholding the Data Protection Act) that young people in the Connexions age range are old enough to be able to make their own decisions about their information, unless there is a reason to suggest otherwise. PAs will need to use their professional judgement to decide if a young person is competent to make such decisions in line with what are known as the 'Fraser Guidelines'. These guidelines were laid down in a court case which concerned contraceptive advice and treatment, but the principle can be extended to other situations. Broadly speaking, PAs need to be satisfied that the young person fully understands the choices they are making and what the potential consequences may be. If a PA has doubts about a young person's ability to provide informed consent then parental consent should also be sought.

6.3 Refusal of consent

If the young person refuses to share sensitive information with another agency then this should be noted on the Core+ IYSS client record that information must not be shared unless any of the conditions in section 7.4 apply. Please also see 6.4.

6.4 Disclosing Information Without Consent

Personal information should only be disclosed for the purpose identified in section 5 and in accordance with what the individual has been told. There are exceptions if the information is required for the following purposes:

- where there are child protection issues involved;
- where there is a significant threat to life;
- where the young person needs urgent medical treatment;
- where potential or actual serious criminal offences are involved;

- where the disclosure is necessary for the prevention of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty or of any imposition of a similar nature (s.29 DPA);
- the disclosure consists of information which is required by law to be made publicly available (s.34 DPA);
- the disclosure is required by law or by order of the court (s.35(1) DPA); or
- the disclosure is made in connection with legal proceedings (s.35(2) DPA).

It is Connexions and Youth Support services **policy** to gain young people's consent to share their information wherever practical. If information sharing is necessary, but the gaining of consent is impractical (e.g. where there has been no contact with the young person for a period of time) information can still be shared between Connexions and Youth Support services. The **legal basis** for sharing without consent in this instance is that it is necessary for the exercise of the Secretary of State's function of providing services under *Section 114 of the Learning and Skills Act 2000*. This in conjunction with the Children Act 2004 section 10, 11 and 12 *(details in Annex A - Guidance to the full legislation);*

These limits to confidentiality should be made clear to young people at the earliest opportunity and where confidentiality has to be broken, PAs should seek to ensure that the young person is informed first or as soon as possible afterwards.

6.5 Further sharing of personal data

Principle 2 of the Data Protection Act 1998 states that "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 these purposes".

The purpose for sharing the data under this policy should be compatible with the provision of Connexions and Youth Support Services. That is, partner agencies can only share information relevant to the services provided for young people, in this case around their learning, training or support. Where the data is being shared for a non-compatible purpose, it is the obligation of the partner agency to seek the permission from the young person for the secondary use of personal data.

6.6 Minimal identifiable information

In line with Principle 3 of the Data Protection Act, "personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed." It is essential that the data collected by partner agencies and that which is shared with other parties is the minimum identifiable information necessary for the purpose of providing appropriate Connexions services to the young person.

6.7 Accuracy of the data

It is the responsibility of each partner agency to ensure and maintain the accuracy of personal information they share with other organisations under this policy. Where an organisation becomes aware that information they have provided may be inaccurate, they must take steps

to inform all partner agencies of the updated data. Information discovered to be inaccurate must be notified to the originating organisation.

6.8 Security of Personal Information

Principle 7 of the Data Protection Act 1998 requires that appropriate measures should be in place to protect the personal information from unauthorised access, loss, damage or destruction.

Partner organisations are responsible for the security of information they hold. Each partner agency must take all reasonable care and employ appropriate physical, technical and organisational safeguards to protect the personal data under this data sharing arrangement. Partner agencies must agree on the standards required for protecting the data, for example, the storage safeguards for information in hardcopy and electronic format, security of data in transmission, security standards for access to the data. As a minimum partner organisations should only allow direct access to their database to staff who have password access to the system. Paper records should be located in a secure filling system that is not accessible to the public and can be locked when not in use. Higher safeguards will be required where the personal data is of a sensitive nature.

Staff of partner agencies should only have access to personal data in order to perform their duties in connection with one or more of the purposes defined in section 5. Technical and physical safeguards should be in place to restrict access to the information only to authorised staff for example, password control.

Partners will have access to aggregated reports as agreed by the West London Partnership Support Unit.
From time to time the West London Partnership Support Unit may commission consultants to undertake research aimed at informing the development of the West London Connexions and Youth Support Service. When contracting with consultants, contacts should specify that all client information used will remain the property of the West London Partnership Support Unit and that during the course of the research the consultant will abide by this information sharing policy.

6.9 Young Person's Access to their Information

Under the Data Protection Act, data subjects have rights to have access to personal information about them held by any organisation. These requests – "subject access requests" - must be fulfilled within 40 calendar days. Each partner agency has responsibility for ensuring that data subjects are informed that they have the right to see a copy of the information it holds and are provided with access to personal information held about them in accordance with the requirements of the Act.

If a young person requests to see their records, they can either be provided with a printed version or show them on screen. This does not have to be immediate but must be provided within 40 calendar days.

6.10 Retention of personal data

Principle 5 of the Data Protection Act 1998 requires that personal data should be kept only for as long as is necessary for the purpose for which it was obtained.

Young people's records will only be kept on the system while they may be of use to the West London Connexions and Youth Support Service. When the young person reaches 20 (or 25 in the case of young people with learning difficulties or disabilities) their records will be archived. This means that their records cannot be viewed by anyone except the systems administrator who would only access theses records if needed for audit purposes by the DfE or European Commission.

Paper records will be disposed of in such a way that they cannot be identified (e.g., by use of a shredding machine). Electronic records will be electronically deleted from the hard drive of the computer system and any back up files. Partner agencies will take responsibility for secure destruction of personal data.

6.11 Recording

When information is received from a source other than direct from the young person the source must be recorded. All requests for information and disclosures must be recorded.

6.12 Third Party Information

A young person may disclose information about a third party that is not relevant to their own learning and development. PAs must not pursue such information unless there is a risk to life or there are Child Protection concerns. Information about third parties must not be recorded in the young person's records unless it is relevant.

7 FURTHER OBLIGATIONS

7.1 Data Controller

Each partner agency remains the "data controller" for the information in accordance with the Data Protection Act 1998.

7.2 Lawfulness Of Processing Of Data

Partner agencies should ensure that the sharing of personal data under this policy is lawful and that the organisation should ensure that it has the appropriate legal power to share the relevant data. Where the organisation's functions are determined by statute (e.g., local authorities or other statutory bodies) these organisations must ensure that they are not acting *ultra vires* in participating in this data sharing arrangement. In addition, partner agency must ensure that the sharing of data meets at least one of the conditions of processing in Schedule 2 of the Data Protection Act 1998.

7.3 Notification under the Data Protection Act 1998

It is the responsibility of each partner agency to ensure that the processing of personal data under this policy is included in their Notification to the Office of the Information Commissioner as required under the Data Protection Act 1998.

7.4 Staff obligations

It is the responsibility of each partner agency to ensure that staff with authorised access to the data covered by this policy are aware of their obligations under the Data Protection Act 1998 and related legislation to safeguard that information. Staff should be aware that breach of this policy could be a matter for disciplinary action and may provide grounds for a complaint under the Data Protection Act 1998 against them which may result in criminal or civil action against them.

7.5 Complaints procedures

Partner agencies should have in place clear and transparent complaints procedures. If any young person is unhappy about how information held about them has been shared by a partner organisation they should be assisted in making a formal complaint to the West London Partnership Support Unit Data Controller in the first instance. Should there be cause to escalate the complaint then this should be done through the Information Commissioner.

8 DECLARATION OF AGREEMENT

I, the undersigned, on behalf of my organisation, agree to provide and keep safe data in accordance with the conditions detailed in this protocol, adhering to relevant legislation as set out in the Data Protection Act 1998.

Name .....

Job title .....

Organisation .....

Address .....

.....

.....

.....

Named contact .....

Telephone .....

Email .....

Named data controller .....

Telephone .....

Email .....

Signature .....

Date .....

9 REVIEW OF THE POLICY

This information sharing policy will be reviewed by the West London Partnership Support Unit annually in line with the business planning cycle. However, such reviews will not prevent ongoing improvement of the systems and methods of data collection and sharing as part of the process of continuous improvement.

10 CONTACT FOR THE POLICY

For all enquiries regarding this policy, please contact:

David Pether
Information Systems & Policy Manager
West London Partnership Support Unit (Connexions)
Perceval House
14-16 Uxbridge Road
Ealing
London
W5 2HL
Tel: 020 8825 9151
Fax: 020 8825 5775
Email: dpether@ealing.gov.uk

Information Sharing Policy for West London Partnership Support Unit and Partnership Agencies

Version issued April 2014