Information Sharing Agreement

London Borough of Barnet

Between LBB [service] and [other organisations]

N.B. All new Information Sharing Agreements must receive sign-off from both Legal and the corporate Information Management Team

Document Control

Document Description	Information Sharing Agreement between the London Borough of Barnet and [other organisations] (to be read in conjunction with and in accordance with the LBB Information Sharing Protocol)		
Version	V.2		
Date Created			
Status	Draft		
Authorisation	Name	Signature	Date
Prepared By:	XXXXXX		20/12/2012
Checked By			

Version Control

Version number	Date	Author	Reason for New Version
0.1	06/12/2012	1.1 XXXXXX	Initial draft
0.2	07/12/2012	1.2 XXXXXX	Amended following discussions with XXXXXX
0.3	12/12/2012	1.3 XXXXXX	Amended following pilot
0.1	20/12/2012	1.4 XXXXXX	Minor amendments following proofing
0.2	22/11/2013	1.5 XXXXXX	Annual Review

Date last reviewed: *November 2013*

Date of next review: *November 2014*

Contents

1 Purpose and scope 3
2 Legal basis for sharing data 3
3 The Data Protection Act and other legislation 4
4 Information being shared 6
5 Commitment / responsibilities of parties involved 6
6 Data handling and security 7
7 Complaints process 9
8 Assessment and Review 9
9 Termination of Agreement 9
10 Signatures and Contacts 9
11 Risk Assessment 11
Appendix A: Information being shared 12
Appendix B: Caldicott Principles 13
Appendix C: Information sharing responsibilities within the authority and partner organisations 14

1 Purpose and scope

1.1 The purpose of this document is to agree the sharing of information between the London Borough of Barnet (hereafter referred to as the "Authority") and [insert other organisations here]

1.2 The Authority and [insert other organisations here] are registered Data Controllers under the Data Protection Act. [You should add the ICO registration numbers of each organisation here]. The partners have established Data Protection and data security policies and procedures in place.

1.3 The sharing of personal data needs to be of benefit to the individual whose information is subject to the agreement. [How will the sharing of information under this agreement benefit the data subjects?]

1.4 [What services will be delivered through the sharing of information under the agreement?]

1.5 [Who are the clients of the services delivered (e.g. age, needs, etc.)?]

2 Legal basis for sharing data

2.1 A Public Authority must have a legal basis for sharing data, and must ensure that all sharing agreements are in compliance with the Data Protection Act 1998.

The Data Protection Act (DPA) 1998

2.2 The DPA 1998 is a framework which allows the safe and legal processing (which includes sharing) of personal and sensitive personal data.

2.3 The DPA 1998 definition of personal and sensitive data is as follows:

2.4 Personal Data – means data which relate to a living individual who can be identified from those data; or from those data and other information which is the possession of, or is likely to come into the possession of, the data controller.

2.5 Sensitive Personal Data - means 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

2.6 The DPA 1998 contains two Schedules that list various conditions which, when satisfied, allow for the processing of personal data (Schedule 2) and sensitive personal data (Schedule 3). These are set out below.

Schedule 2, DPA 1998

2.7 Schedule 2 of the DPA sets out the conditions for the processing of personal data. At least one condition must be met in order to legitimately process personal data.

2.8 [What conditions are met that will allow personal data to be shared under Schedule 2 of the DPA?]

2.9 However, the actual disclosure of any data to achieve these objectives must be conducted within the framework of the DPA, Human Rights Act (HCA) and Caldicott Principles as well as with regard to the Common Law Duty of Confidence. It is also subject to any express prohibition in legislation.

Schedule 3, DPA 1998

2.10 If the information is "sensitive" as defined by the DPA 1998 you must in addition to satisfying a Schedule 2 condition also satisfy **at least one** condition in Schedule 3.

2.11 [What conditions are met that will allow sensitive data to be shared under Schedule 3 of the DPA?]

3 The Data Protection Act and other legislation

3.1 The disclosure of information is subject to a legal framework including DPA, Human Rights Act and Caldicott Principles amongst other legislation. The most significant are outlined below.

The eight principles of the data protection act

3.2 There are 8 DPA principles must be complied with. These are set out below.

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.*

Freedom of Information (FOI)

3.3 The Freedom of Information Act gives all individuals the right to access official information held by a public authority. Limited exemptions may apply and all public authorities must ensure they have recognised procedures in place for administering requests of this nature. Public authorities have a statutory responsibility to reply to requests within 20 working days.

3.4 All requests for FOI will be directed through the FOI Administrator in the Authority in the first instance. Advice will be sought through partner organisations where there is concern about that information being released and any impact it is likely to have. The final decision to disclose or not will lie with the authority who holds the information.

3.5 This document may also be disclosed to the public under the FOI Act.

Subject Access Requests (SAR)

3.6 Each organisation must have a recognised procedure in place to handle subject access request made under the Data Protection Act 1998.

3.7 Under the Act individuals (“Data Subjects”) have the legal right, subject to some exemptions, to information about themselves that is held by the Authority. The request (“Subject Access Request”) has to be made by the Data Subject in writing.

3.8 Subject access requests will in the first instance go through the Authority lead who will collate information requested unless it falls under any of the exemptions that allow it to be withheld. Where there are concerns regarding the release of health information advice will be obtained from health information governance departments in the relevant partner organisation

3.9 Once the Authority has received a valid request the timescales and guidance under the policy will apply. Responses to any subject access requests will be prompt and in any

event will be sent within the statutory 40 calendar days from when both identification confirmation and payment (if applicable) have been received from the Data Subject

3.10 Personal data may be withheld from disclosure in limited circumstances and only in instances where if it falls under any of the exemptions described in the Act. Further information regarding the Act can be found on the Information Commissioner's Officer's website www.ico.gov.uk.

3.11 **Please refer to the Authority's Subject Access Procedure for more information**.

4 Information being shared

4.1 Appendix A sets out the personal data being shared between partners, it details: -

- What data is being shared
- Who in the organisation shares the data
- How is the data shared, including the security measures applied
- Who in the organisation receives the data
- What happens with the data when it is received
- Any retention periods applied to the data

4.2 These arrangements must be reviewed every six months to ensure that the benefits to the data subjects are being realised. All parties agree that data sharing of personal and sensitive personal data must not be entered into purely for the administrative benefit of the organisation.

5 Commitment / responsibilities of parties involved

5.1 Every individual working for the partners listed in this Agreement are personally responsible for the safekeeping of any personal and sensitive personal data they obtain, handle, use and disclose.

5.2 It is the responsibility of each partner to ensure that every employee knows how to obtain, use and share personal data in line with the Data Protection Act 1998. Mandatory training provided by the relevant partner organisations must be undertaken once a year to ensure responsibilities are clear and up to date. The Authority [and other organisations party to this agreement] will provide training regarding data protection and information sharing arrangements to the respective staff in their organisation that will access the information under this agreement, through the line management structure. All new staff and staff new to the relevant policies whether permanent, contracted or temporary will have data protection and local information sharing agreements training as part of their induction and noted in supervision documentation.

5.3 Every individual must uphold the principles of confidentiality, follow the guide-lines set out in the London Borough of Barnet Information Sharing Protocol and seek advice when necessary. Caldicott Principles apply to all information sharing and data should only be shared in accordance with these principles (see Appendix B).

6 Data handling and security

6.1 The clauses below outline the duties of all parties in regards to handling information.

Capture

6.2 All parties will implement the necessary privacy notices and obtain appropriate consent from data subjects at the point at which personal data is captured, in order to adhere to the DPA principle of 'fairly and lawfully' processing data. These notices will inform the data subject that the information will be shared with the parties under this agreement and the purposes for which it will be shared.

6.3 In circumstances where a data subject whose data has previously been shared between partners withdraws their consent, the party that has been informed by the subject will communicate this to the other partners. In each case those partners that no longer have consent to access this information will be responsible for securely disposing of such information.

Security management

6.4 It is the responsibility as signatories to this Agreement that parties ensure that they have appropriate technical and organisational security measures in place to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

6.5 London Borough of Barnet works towards ISO 27001, the International Standard for Information Security Management. There is an expectation that partner organisations will either be working towards the same or a similar standard of security.

Secure sharing of information

6.6 [In this section you should consider how information will be shared (see table in Appendix A) and what implications this will have in terms staff behaviour, administration, etc. The following clauses on email transfer can be amended to meet circumstances]

6.7 Email is not generally a secure method of transferring patient data and patient data should not be transferred via email except via the following approved, secure methods.

6.8 All sensitive data must be sent via [insert the appropriate type of secure email here] email.

6.9 Any transfers of personal data or personal identifiable data (PID) must be appropriately packaged and securely transferred, to mitigate any loss or unlawful disclosure of data.

Access management

6.10 All appropriate staff having access to the data will be enhanced CRB vetted [or equivalent appropriate method] and anyone no longer required to have access will promptly have such access revoked by the line manager and Human Resources related to the relevant employer.

6.11 For [insert relevant organisations here] staff employed through partner organisations, LBB ID passes are worn at all times in Authority facilities in order to ensure access to the premises is legitimate and any person without ID can be challenged regarding their authority.

Data retention and disposal

6.12 Partners must comply with the Authority's policy on data retention and disposal when handling data originating from LBB. For the client group concerned this means securely retaining personal data until required under Records Management Policy after which the data should be securely disposed of.

6.13 All data held by partner organisations electronically will be stored in a secure network area with password protected entry and appropriate back-up functionality. The system will be auditable so that it is possible for any auditor to establish who has accessed the system. All laptops, computers, and any other portable devices will be encrypted.

6.14 If data is printed off an electronic system it will be the responsibility of each organisation to safely dispose of paper records by using a cross cut shredder. The printing of paper copies must be kept to a minimum and only removed from site if there is a genuine business need and data can not be accessed in a more secure manner.

6.15 Any paper records printed must be kept to a minimum and kept secure at all times whether in the office, home or during transit. Appropriate security methods must be applied and paper records must be stored separately from any computers, laptops, personal belongings or other such valuables.

Data breaches

6.16 All partners must have a clear policy and procedure in regards to the reporting and handling of data protection breaches or data loss incidents. Where data loss is in connection with [insert relevant services delivered under the agreement here] this must be reported in the first instance to Data Protection Officer and a decision made whether the incident is investigated jointly with the partner organisations. All staff will adhere to the protocols/ policies and procedures of the Authority but line managers must inform the respective information governance departments in the partner organisations that an incident has been recorded.

6.17 All new staff will be inducted into the locally agreed information sharing governance procedures and training will be provided to all existing staff not already familiar with the agreement

7 Complaints process

7.1 Partner organisations must ensure they have clear, fair and objective procedures in regards to the handling of complaints. Any complaints raised in relation to the [insert the relevant LBB lead here], must be managed in the first instance by the Authority and where necessary the lead for complaints will communicate with the other partner organisations. Where there are professional issues/concerns the relevant partner organisation should lead on any investigation in partnership with the Authority.

8 Assessment and Review

8.1 A review of the information sharing agreement will take place every six months after the agreement date of this document through the [insert the owner of this agreement], who has responsibility for the governance of the agreement. This will assess the success of the agreement and the procedures followed for effective information security management. Changes in legislation and developments in the areas of public sector data sharing will be taken into account if and when they arise.

8.2 During the review all elements of the sharing agreement must be addressed and checked for compliance. The aim of the review will be to ensure the scope and purpose are still relevant and the scope has not slipped and the benefits to the data subject are being realised. The review must ensure that the data subjects are still the focus of the sharing arrangement and the arrangement is still benefiting the individuals whose data is being shared.

9 Termination of Agreement

9.1 The agreement will expire or terminate in line with the contract between the Authority and [relevant organisations].

9.2 In the event of termination of this agreement each party may continue to hold information originating from other parties. This information will continue to be handled in line with the originating parties' policies regarding information management.

10 Signatures and Contacts

10.1 This agreement lays down procedures that provide a secure framework for the sharing of data between signature agencies in accordance with statutory and professional responsibilities. Nevertheless, signatory agencies accept that it is their responsibility to ensure their actions are lawful and to obtain any independent legal advice

10.2 We the undersigned agree that the organisation that we represent will adopt and adhere to this information sharing agreement:

Organisation	Role	Name	Signature	Date

11 Risk Assessment

An assessment of the risks involved in sharing and handling the information should be undertaken in order to identify the instances where a data breach or misuse of data is most likely.

Actions to mitigate the risks of a data breach in these instances should be developed and implemented.

These risks should be incorporated in the LBB Service Risk Register where appropriate.

Risk	**Likelihood (1 – 5)**	**Severity of Impact (1 – 5)**	**Overall Risk (1 – 25)**	**Mitigation**

For more information on identification and assessment of risks please refer to the LBB Risk Management Framework.

Appendix A: Information being shared

What information is being shared	Who in the organisation shares the information	How is the information shared	Who in the organisation receives the information	What happens with the information when it is received	What retention period is being applied to the data
	e.g. Social Worker	e.g Secure email (GCSX to GCSX/GSI)	e.g. DWP Disability Employment Advisers	e.g. stored in DWP database, used to validate benefits claims, retained for 5 years before secure disposal	

Appendix B: Caldicott Principles

1. Justify the purpose(s) of using confidential information

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

2. Do not use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary patient-identifiable information that is required

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

4. Access to patient-identifiable information should be on a strict need-to-know basis

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

5. Everyone with access to patient-identifiable information should be aware of their responsibilities

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

6. Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with the legal requirements.

Caldicott Guardians are senior staff in the NHS and social services appointed to protect patient information..

Further information can be found in the Caldicott Guardian Pages on the Department of Health web site.

Appendix C: Information sharing responsibilities within the authority and partner organisations

Named Officer	Responsibility	Organisation	Contact Details	Review and comments
	e.g. Service Manager, Data Protection Officer, Caldicott Guardian, FOI/SARS lead			