Merton Mencap

Data Protection, Confidentiality and Security of Information

Policy and Procedure

April 2014

Merton Mencap

Data Protection, Confidentiality & Security of Information POLICY & PROCEDURE

This policy and procedure has been adopted by Merton Mencap through its Executive Committee which remains responsible for its review.

Original signed version is kept at the Merton Mencap office.

Signed: _____ Date: _____

Name: _____

Chair of Executive Committee

Signed: _____ Date: _____

Name: _____

Chief Executive

Record of adoption and review of this policy and procedure:-

Adopted: 28 June 2011
Reviewed: 29 April 2014

Merton Mencap

Data Protection, Confidentiality and Security of Information

Policy and Procedure

A. Definitions

For the purposes of these policies and procedures:-

1. *DPA* means the Data Protection Act 1998, and the following terms have the meanings given to them in the *DPA*, as summarised in **appendix 1** below:-

   personal data
   sensitive personal data
   data controller
   data subject
   data protection principles
   right of subject access

2. *Staff and staff member* includes Merton Mencap employees, bank workers and volunteers

3. *Personal information* means any information relating to an individual from which that individual can or may be identified, whether or not it is also within the definition of *personal data*

4. *Financial information* means any information not already public relating to the finances of Merton Mencap

5. *Sensitive information* includes *sensitive personal data* within the meaning of the DPA and, whether or not it is also within any other definition above, also includes:-

   - any information, which is not already public and which, due to its nature, is clearly not appropriate to be shared with others, and
   - any information which is not already public and is shared in a relationship where the person giving it understood or would reasonably expect that, due to its nature, it would not be shared with others

6. *Consent* - Whether any consent required has been given will depend upon the circumstances of the particular case. In cases of uncertainty, staff should seek guidance from the Chief Executive.

B. Scope of these Policies and Procedures

1. The provisions in these policies and procedures are in addition to all other provisions relating to data protection, confidentiality and security of information in other policies and procedures of Merton Mencap, in any code of conduct of Merton Mencap or in any terms and conditions of employment or of any contract with Merton Mencap. All staff are required to comply with these provisions both during and after termination of their working relationship with Merton Mencap.

2. Nothing in these policies or procedures in intended to adversely affect the operation of Merton Mencap's Whistle Blowing Policy & Procedure.

C. Data Protection

1. General

The DPA provides a framework to ensure that certain personal information is handled properly, in an attempt to ensure a balance between the needs of organisations to collect and use personal information, for business or other purposes, and the rights of individuals to privacy of their personal details. **A brief summary of key provisions is contained in appendix 1 below, by way of guidance for the purposes of these policies and procedures**.

2. Data Protection Policy

Merton Mencap is fully committed to complying with all its legal obligations relating to data protection and with relevant codes of practice.

3. Data Protection Procedures

3.1 The Role of the Chief Executive

In cases of uncertainty as to the application or effect of any provisions of the DPA in any given situation, advice must be sought. Staff are asked to refer any queries to the Chief Executive, who has day to day responsibility for ensuring Merton Mencap's compliance with the legislation.

3.2 Merton Mencap as a *data controller*

Merton Mencap is notified with the Information Commissioner's Office as a *data controller* under registration no Z6270805.

As a *data controller* Merton Mencap is required to ensure that all *personal data* is dealt with in accordance with the 8 *data protection principles*. These terms are explained further in **appendix 1 below.**

All staff are required to be familiar with the meaning of *personal data, sensitive personal data* and with the *data protection principles* and to comply with those principles to the extent appropriate to their level of responsibility.

In this context, all staff are also required to comply with the procedures referred to in **sections D and E** below on **Confidentiality** and **Security of Information**.

3.3 Requests under the *right of subject access*

Any staff member receiving any request which is or may be a request under *the right of subject access* must immediately refer the request to the Chief Executive.

D. Confidentiality

The provisions of this section D are *in addition* to the provisions section C above and section E below.

1. Confidentiality Policy

It is the policy of Merton Mencap to keep confidential all personal information, financial information and sensitive information.

2. Confidentiality Procedures

2.1 Personal Information

Personal information, whether in hard or soft copy form, for example, names and contact details of service users and details of their needs, should only be accessed by staff to the extent necessary for the performance of their duties in working with Merton Mencap.

Personal information, whether in hard or soft copy form, should not be held by any staff member outside Merton Mencap's offices, save to the extent necessary for the carrying out of Merton Mencap's business or activities in a lawful, proper and efficient manner. *Personal information* so held is the responsibility of the individual holding it.

Personal information, whether in hard or soft copy form and wherever held, should not be left unattended when in use and must be stored securely when not in use.

Any loss of *personal information*, in whatever form*,* must be reported as soon as practicable to the Chief Executive, or, in his absence, the Chair of Trustees.

Personal information, in whatever form, must not be disclosed to anyone outside Merton Mencap save as referred to in [2.4] below.
Further details on procedures are contained in section E below.

2.2 Financial information

Financial information, whether in hard or soft copy form*,* should only be accessed by staff to the extent necessary for the performance of their duties in working with Merton Mencap.

Financial information, whether in hard or soft copy form, should not be held by any staff member outside Merton Mencap's offices, save to the extent necessary for the carrying out of Merton Mencap's business or activities in a lawful, proper and efficient manner. *Financial information so held* is the responsibility of the individual holding it.

Financial information, whether in hard or soft copy form and wherever held, should not be left unattended when in use and must be stored securely when not in use.

Any loss of *financial information*, in whatever form, must be reported as soon as practicable to the Chief Executive, or, in his absence, the Chair of Trustees.

Financial information, in whatever form, must not be disclosed to anyone outside Merton Mencap save as referred to in [2.4] below.

Further details on procedures are contained in section E below

2.3 *Sensitive information*

Sensitive information, whether in hard or soft copy form*,* should only be accessed by staff to the extent necessary for the performance of their duties in working with Merton Mencap.

Sensitive information, whether in hard or soft copy form, should not be held by any staff member outside Merton Mencap's offices, save to the extent necessary for the carrying out of Merton Mencap's business or activities in a lawful, proper and efficient manner. *Sensitive information* so held is the responsibility of the individual holding it.

Sensitive information, whether in hard or soft copy form and wherever held, should not be left unattended when in use and must be stored securely when not in use.

Any loss of *sensitive information*, in whatever form, must be reported as soon as practicable to the Chief Executive, or, in his absence, the Chair of Trustees.

Sensitive information, in whatever form, must not be disclosed to anyone outside Merton Mencap save as referred to in [2.4] below.

Further details on procedures are contained in section E below

2.4 Disclosure of information outside Merton Mencap

Personal information must not be disclosed outside Merton Mencap unless those to whom it relates gives their *consent* or its disclosure is required by law or other regulatory requirements, and see further on *sensitive information* below.

Financial information must not be disclosed outside Merton Mencap, without the consent of the Chief Executive, the Chair of Trustees or the Treasurer, or as required by law or other regulatory requirements.

Sensitive information must not be disclosed outside Merton Mencap unless those to whom it relates give their *consent* or its disclosure is required by law or other regulatory requirements, and see further on *sensitive information* below.

2.5 Sharing *sensitive information*

In the context of safeguarding children and safeguarding vulnerable adults from abuse, *sensitive information* may need to be shared as provided for in:-

Merton Mencap's Safeguarding Children Policy and Procedure
Merton Mencap's Safeguarding Adults at Risk Policy and Procedure

Staff should refer to the relevant policy and procedure if they feel *sensitive information* needs to be shared in any given case. In any event, save in cases of emergency, staff must refer to the Chief Executive, as the nominated safeguarding children adviser or the responsible person for safeguarding vulnerable adults, for guidance**.**

2.6 Avoiding casual disclosure of information

All staff are required to take all reasonable measures to ensure that:-

- when using any *personal information, financial information or sensitive information,* in whatever form and in whatever circumstances, such information is not seen by any person who is not authorised to see it, and
- when discussing any *personal information, financial information or sensitive information,* in whatever circumstances, such information is not heard by any person who is not authorised to hear it.

2.7 Return of all documentary information

All documentary information, whether in hard or soft copy form, given to or acquired or created by any staff member in the course of and relating to their working with Merton Mencap must be returned to Merton Mencap at the end of the working relationship.

E. Security of Information

The provisions of this section E are in addition to the provisions sections C and D above.

1. Security of Information Policy

It is the policy of Merton Mencap to have in place operational measures to ensure that information relating to its business and activities is kept secure and in a manner consistent with relevant law, regulatory requirements and recommended practice.

2. Security of Information Procedures

2.1 Responsibilities

The Chief Executive has day to day responsibility for security measures. All staff members are responsible for ensuring that all *personal information, financial information and sensitive information* with which they may come into contact in their work with Merton Mencap is kept secure by them in accordance with these policies and procedures, and are required to report any matters of concern relating to the security of such information to the Chief Executive as soon as practicable.

2.2 Information in hard copy form

Personal information, financial information and sensitive information in hard copy form, wherever held, is required, when not actively being used, to be kept in locked drawers/filing cabinets/cupboards, with access to relevant keys and knowledge of their location being restricted to staff who may need access to such information to carry out their duties.

All such information when being taken from one place to another is required to be kept under the direct control of the person responsible for it in as secure a manner as is practicable in all the circumstances.

No such information should be posted unless authorised by the relevant projects manager, the Chief Executive, Chair of Trustees or the Treasurer for the efficient running of Merton Mencap's business and activities. Original

documents of which no copy exists should, wherever reasonably practicably, be copied before posting.

2.3 Information in soft copy form

Personal information, financial information and sensitive information in soft copy form, wherever held, must be subject to password access for individual authorised users only, authorisation being restricted to staff who may need access to such information to carry out their duties.

All such information when being taken from place to place, in particular on any portable equipment or media (such as laptops, tablet computers, memory sticks and memory cards), is required to be kept under the direct control of the person responsible for it in as secure a manner as is practicable in all the circumstances.

Equipment or media containing any such information must not be posted under any circumstances.

2.4 Retention and disposal of information

Personal information, financial information and sensitive information, in whatever form, will be held for such period, depending on its nature, as complies with recommended practice on retention of information. In particular, information relating to any safeguarding issue will be kept indefinitely and *financial information* will be kept for a minimum of 7 years.

On any disposal, p*ersonal information, financial information and sensitive information* in hard copy form will be shredded

On any disposal, p*ersonal information, financial information and sensitive information* in soft copy form will be deleted from the relevant equipment and media.

Equipment and media which has contained p*ersonal information, financial information or sensitive information* will be disposed of in such manner as ensures that any residual information is securely deleted in the disposal process.

2.5 Office Security

The entrance door to Merton Mencap's offices within the Wilson Hospital is kept locked at all times when no staff member is working in them. Access to the relevant key code is restricted to staff members needing access to the offices to carry out their duties, and others authorised by the landlord, Sutton & Merton PCT, for specific purposes under leasing arrangements agreed with the PCT.

The entrance door to the Chief Executive's office at Merton Mencap is kept locked at all times when neither the Chief Executive nor any staff member authorised by him is working in it. Access to the relevant key code is restricted to staff members needing access to the office to carry out their duties, and others authorised by the landlord, Sutton & Merton PCT, for specific purposes under leasing arrangements agreed with the PCT.

2.6 Specific arrangements

The precise arrangements showing, in detail, how Merton Mencap manages the provisions set out in this policy are set out in a separate, operational document, titled '*Merton Mencap – arrangements to ensure data protection'.* Due its nature, that document does not form part of this policy and is only available to Merton Mencap management.

Merton Mencap
Data Protection, Confidentiality and Security of Information
Policies and Procedures

Appendix 1
The Data Protection Act 1998

This Appendix contains a brief summary of key provisions of the DPA for the purposes of these policies and procedures. Further reference should, however, always be made to the detailed provisions of the Act. The Information Commissioner's Office, which enforces and oversees the DPA, issues guidance on the DPA, see www.ico.gov.uk. In cases of difficulty or uncertainty, legal advice may be needed.

1. The DPA applies to *personal data*

Data means information held or intended to be held on a computer **or** in a *relevant filing system,* and a *relevant filing system* means where information is structured in such a way that specific information about an individual is readily accessible. D*ata* can include video recordings and photographs.

Personal data means data about a living individual who can be identified directly or directly from the data held or likely to be held. It can include indications of intention or expressions of opinion.

Sensitive personal data means personal data relating to the racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, proceedings for any offence committed or alleged to have been committed, or the disposal of such proceedings or the sentence of any court in such proceedings.

2. The DPA regulates the *processing* of *personal data*

Processing, means obtaining, recording or holding the data or carrying out any operation on it, including organising, adapting or altering it, retrieving, consulting or using it, disclosing it or otherwise making it available, and destroying it.

3. The DPA imposes duties on *data controllers* and gives rights to *data subject*s

A *data controller* is an individual or organisation who decides, whether alone or with others, how *personal data* are processed and for what purposes

A *data* subject is an individual who is the subject of *personal data*

4. A *data controller* must process *personal data* in accordance with 8 *data protection principles*

The *data protection principles* are broadly:-

1. Personal data must be processed fairly and lawfully. In particular, at least one of the conditions for processing referred to below has to be met and, in the case of sensitive personal data, at least one of further conditions for processing referred to be below has to be met.

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

3. Personal data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

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

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

6. Personal data must be processed in accordance with the rights of data subjects.

7. Measures must be taken shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage.

8. Personal data must not be transferred to countries outside the European Economic Area unless adequate levels of protection exist in the relevant country.

5. At least one of specified *conditions for processing* must be met for the processing of *personal data*

These conditions include, in summary:-

- the individual concerned has consented to the processing.
- the processing is necessary in relation to a contract which the individual has entered into, or because the individual has asked for something to be done so they can enter into a contract.
- the processing is necessary because of a legal obligation on the data controller (other than a contractual one).
- the processing is necessary to protect the individual's "vital interests" - this condition only applies in cases of life or death.
- the processing is in accordance with the "legitimate interests" condition.

The *legitimate interests* condition requires a balancing of competing interests.

6. At least one of specified further *conditions for processing* must be met for the processing of *sensitive personal data*

These conditions include, in summary:-

- the individual concerned *has given explicit consent* to the processing.
- the processing is necessary so that the data controller can comply with employment law.
- the processing is necessary to protect the vital interests of the individual (in a case where their consent cannot be given or reasonably obtained), or another person (in a case where the individual's consent has been unreasonably withheld).
- the processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents - extra limitations apply to this condition.
- the individual has deliberately made the information public.
- the processing is necessary in relation to legal proceedings, for obtaining legal advice, or for exercising legal rights.
- the processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

Consent is not defined in the DPA. However, guidance is available from the Information Commissioner's Office as referred to above.

7. A *data subject* has a *right of subject access*

Subject to certain exemptions, an individual is entitled, on written request, to be:-

- told whether any personal data is being processed;
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

An individual is entitled only to their own personal data and not to information relating to another individual.

Such a request must be responded to promptly and in any event with 40 days. A fee not exceeding £10 can be charged for dealing with the request.

Check	Evidence
Staff know which Act underpins the rules for managing data	Ask staff (either 1:1 Oor in group setting)
Staff are aware what personal data and sensitive personal date is	Ask staff (seek examples)
Staff know what their responsibilities are in relation to the following provisions within this document: **D: Confidentiality** - 2.4 - 2.5 - 2.6 - 2.7 **E: Security of Information** - 2.2 - 2.3 - 2.4 - 2.5	Ask staff Observations in the office