Merton Mencap

Data Protection, Confidentiality and Security of Information

Policy & Procedure

July 2017

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

Reviewed: 25 July 2017

Data Protection

From May 2018, data protection law will be determined by the GDPR (General Data Protection Rule), a European Law that is expected to become enshrined in UK law prior to our leaving the European Union. After May 2018, the current Data Protection Act 1998 and The Privacy and Electronic Communications (EC Directive) Regulations 2003 will be replaced by the GDPR.

This policy aims to be compliant with the GDPR as far as possible although this policy will be reviewed and updated again once the new UK legislation has been passed into law. This policy is also intended to comply with existing data protection legislation.

What does it apply to?

Data protection principles must be enshrined in the charity's people (in terms of culture and training), processes (how we do our business each day) and technology (how we use electronic and mobile technology to store and use data).

Data protection rules relate to **personal data** with sensitive personal data requiring additional rules and safeguards. Personal data is any data relating to an identifiable, living individual. This includes name, address, personal attributes, characteristics, behaviours, habits, preferences and choices. This also includes our unique identifiers such as NHS number, National Insurance number and potentially a database ID number, the IMEI number of our phone and IP address of our personal computer.

Sensitive personal data includes disability, ethnic background, political opinions, trade union status, religious beliefs, health, sexual health and criminal records.

Under the law, Merton Mencap is a data controller for all personal data we hold regarding our employees, volunteers, clients, clients' families, and also many of our members, supporters, commissioners, and donors.

Merton Mencap Policy

Data Protection Officer

The Chief Executive is the organisation's Data Protection Officer and is responsible for ensuring that all staff and volunteers are aware of their responsibilities under data protection law and for ensuring that Merton Mencap complies with current data protection law (whether or not the current law is properly reflected in this policy).

Access to personal data

Any person for whom we hold or may hold personal data can request that they see a copy of the information stored. We will comply with any such request within 30 days.

If the person asks us to correct or update the data we hold, we aim to do this with 5 days of the request.

Lawful, fair and transparent with consent

Job applicants, employees and volunteers

Personal information received during a recruitment process will be destroyed by Merton Mencap's Office Administrator (via the NHS confidential paper bins) once a selection is made and the person selected has signed the contract for the role concerned. In the event of that we may wish to contact an unsuccessful applicant again if another position becomes available in the future, we will ask for permission to retain personal information for a further period which will be defined at that time.

The application pack of the successful applicant/employee will be retained as part of their HR file which subsequently will contain staff appraisal information and any other HR information which is necessary for the efficient operation of our management and supervision processes. Staff may ask to see their HR file at any time. Consent to hold this information is given when they sign their employment contract. HR files are kept securely in locked cabinets which are themselves stored in locked offices during non-working hours, the offices are accessible via a secure key pad and the code is known only to Merton Mencap staff and key building maintenance staff (for security purposes).

Once a person leaves our employment, we retain their information on our accounting system for a minimum of 7 years after their departure for audit purposes and in order to process any queries relating to their pensions or other payments. The person's hard copy and/or electronic HR file is also retained for 7 years, after which time it will be deleted or destroyed. We have an electronic record of the dates when a person's HR information should be destroyed. This is checked twice per year during an internal audit process.

Volunteer information comprises the data they give us at the recruitment stage plus information such as training courses completed, DBS checks approved and performance data. We will destroy volunteer information within 5 years of a volunteer formally leaving us. We retain information for this period in case they decide to return or in case a query arises about a particular incident at a service. It also enables us to find the volunteer's role and performance details in the event that they ask us for a job reference.

Clients and their families

Children, young people or adults using our services and their parents or carers provide personal details prior to attending a service. Normally this is via a paper or an electronic form although it could be provided verbally.

The information should enable staff to communicate with the person and their family, handle emergencies, arrange transport, report on aspects of Merton Mencap's performance to funders (including sensitive personal information such as type of

disability and ethnicity), and implement safe care whilst the person is with us. This may include personal care, medication, moving and handling information, equipment needs, and, in some cases this includes holding the content of statutory reports such as Education, Health and Care Plans, medical reports, physiotherapy reports, occupational therapy reports and psychology reports. We also hold financial data if a person needs to pay club subscriptions or if the person pays for their own service via a person budget. The purpose of all data we hold is either to deliver the best possible services to clients or to report effectively to funders on how well we are meeting their required performance targets.

Merton Mencap will never sell personal information to a third party or provide it to a third party for any purpose unless we are legally obliged to for safeguarding purposes or as part of a criminal investigation.

We may provide anonymous or summarised data to organisations for academic research purposes.

Whilst we do not ask for a person's data directly for fundraising reasons, we reserve the right to communicate with our clients in a reasonable, polite and responsible way about such matters e.g. sending out membership requests, newsletters, information that they may find interesting (such as the Merton Mencap Annual Report) and information about the charity's work which could help people to raise funds on our behalf, if they so wish, such as our Just Giving weblink or a crowd-funding request that they may wish to pass on to their own contacts.

Merton Mencap will never pressurise clients, their families or other contacts into carrying out fundraising against their wishes and we will not ask for donations in a way that is likely to make a person feel uncomfortable. All donations to Merton Mencap are 100% optional.

Other personal data

We hold the contact details for some funders, potential funders and commissioners, some of whom may be individuals (such as major donors). We obtain this information from the individual concerned ensuring that they provide us with written authority for us to contact them for the purpose of fundraising.

Will do not intend to buy donor information from a third party, however, if this situation arises, we will not send fund-raising requests unless we have firm evidence that the person has given their express, written permission for this to occur.

We may hold the bank details of our current funders or other sensitive personal information, if necessary for funding purposes. We will delete or destroy all data with 5 working days of the person requesting this. We will routinely remove all such information from our systems and hard copy files as soon as it is clear that Merton Mencap no longer will need to use it for the purpose for which it was originally provided.

Specified, explicit and legitimate purpose

All data collected for specified, explicit and legitimate purposes will not be further processed in a manner that is incompatible with those purposes. Any use for scientific or historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes.

Adequate, relevant and limited to what is necessary

Merton Mencap will hold personal data that is adequate, relevant and necessary for the purposes for which it is being processed. This purpose will be recorded at the time that the data is requested or received. Any individual can ask at any time for what purpose we intend to use their information.

Accurate and up to date

Merton Mencap aims to hold accurate and up to date information and we take every reasonable step to ensure that personal data is reviewed and updated, as necessary.

Kept for appropriate periods

Merton Mencap keeps data in a form which permits identification of data subjects for as long as is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods in so far as the personal data will be processed solely for scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by law in order to safeguard the rights and freedoms of individuals.

Security

Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Merton Mencap may choose to hold personal data in an IT system stored off-site, for example with a cloud provider. We will ensure that there are appropriate contractual terms in place to ensure full security of personal data and these terms will be made available to individuals upon request. If implemented correctly, off-premises data storage can offer the same or better security than on-premises solutions. We will take all necessary steps to ensure that this is the case and will make security of personal data the highest priority when deciding on any IT system or process.

Staff and Volunteer Training

All staff and volunteers sign a confidentiality statement prior to starting work for Merton Mencap. A key element of the staff code of conduct and our volunteer agreements is the requirement for staff and volunteers to follow the law relating to data protection as well as Merton Mencap's own policy and procedures relating to confidentiality and the handling of personal data. Failure to do so may result in disciplinary action. A serious breach of security, e.g. putting a client's personal data

at risk, would be cause for summary dismissal *(please see Merton Mencap's Disciplinary and Capability Policy and Procedure).*

Staff will receive data protection and confidentiality training during their induction period and will receive regular briefings with regard to security procedures both in the office and off site. This will be updated periodically a staff meetings and at refresher training sessions. Staff must ensure that they are particularly vigilant if they have responsibility for updating, storing or transporting personal information e.g. holding care plans at project sessions.

Data Protection Procedures

The Role of the Chief Executive

In cases of uncertainty 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.

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 data protection principles.

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 below on Confidentiality and Security of Information.

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.

Confidentiality

Confidentiality Policy

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

Confidentiality Procedures

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 or visible in a public place when in use and must be stored securely when not in use. For example, care plans for use at a project session will need to be accessible to all staff, if needed, but should be kept out of sight and not within easy reach of clients or their families.

They should be stored in a place and manner such that they cannot be accidentally moved or mistakenly taken by others, such as school security staff. If possible, there should be a secure cupboard or drawer at each setting for this purpose which can be locked or otherwise safely protected.

Any loss of personal information or suspected loss of 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 below.

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 below.

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 or visible in a public place when in use and must be stored securely when not in use. For example, care plans for use at a project session will need to be accessible to all staff, if needed, but should be kept out of sight and not within easy reach of clients or their families.

Sensitive information should be stored in a place and manner such that this cannot be accidentally moved or mistakenly taken by others, such as office security staff. If possible, there should be a secure cupboard or drawer at each setting which can be locked or otherwise safely protected.

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 below.

Disclosure of information outside Merton Mencap

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

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.

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.

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.

Security of Information

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 current law, regulatory requirements and recommended practice.

Security of Information Procedures

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 the law and

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.

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.

When in use, this information should be out of sight, and if possible, in a locked or secured place where there is minimal chance of clients, clients families or others (the general public, security staff) being able to remove it, whether accidentally or on purpose.

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. This would normally mean a zipped bag or container with Merton Mencap's contact details clearly marked, so that it can be returned easily in case of accidental loss.

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.

Information held electronically

Personal information, financial information and *sensitive information* in electronic form 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. All smart phones, laptops and tablets must have a secure password or code that is necessary to turn on and use the device in addition to the passwords needed prior to using any online IT system and the passwords attached to the files or data storage system themselves.

Passwords must not be changed by staff without informing the Office Manager at the same time. The Office Manager must have a record of all passwords used for all Merton Mencap devices that contain this kind of information.

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

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.

Personal information, financial information and sensitive information in hard copy form will be shredded or disposed of in confidential waste bins provided by the NHS or Local Authority for such purposes.

Personal information, financial information and sensitive information held electronically will be deleted from the relevant equipment and media.

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

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 all offices at Merton Mencap are kept locked at all times when the staff members authorised to use them are not working in them. Access to the relevant key codes are 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.

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.

Internal Audit Guidance

Check	Evidence
Staff know which Act underpins the rules for managing data	Ask staff (either 1:1 or 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:	Ask staff Observations in the office