****

**Data Protection Policy**

**Aims of the policy**

* To safeguard staff, volunteers, service users and carers and supporters by ensuring that personal information is handled appropriately.
* To ensure Sutton Mencap complies with its legal obligations under the General Data Protection Regulation.

**Introduction**

The General Data Protection Regulation (GDPR) covers information about individuals which is held on computer or in a manual filing system, or which is recorded with the intention that it will be part of such systems. The Regulation applies to people or organisations that use or hold such personal data.

The Regulation is based on the right of the individual (the Data Subject) to know what information is being held about them, and how the information will be used. The Regulation set out principles to ensure that personal data is:

* processed fairly and lawfully
* obtained only for specified purposes
* relevant to the purposes for which it is processed
* accurate and kept up to date
* not kept for longer than is necessary
* processed according to the rights of the Data Subject under the Regulation
* protected against unauthorised processing, accidental loss or damage
* not transferred to areas outside of the European Union (including via websites)

Sutton Mencap holds personal information on volunteers, staff, service users and carers and supporters. As such, Sutton Mencap is defined as a ‘data controller’. This means that we determine the purpose and means of the processing of your personal data. In managing this information, Sutton Mencap seeks to comply with both the letter and the spirit of the Regulation.

We need to gather and use information or ‘data’ about individuals as part of our business and to manage our relationships. We are committed to complying with our all the Data Protection legal obligations

The security and privacy of individual’s data is taken seriously by Sutton Mencap. We have taken steps to protect the security of individual’s data and will train staff about their data protection responsibilities as part of the induction process. We will only hold data for as long as necessary for the purposes for which we collected it.

The policy should be read alongside any contract of employment or contact for services and any other notice we issue from time to time in relation to an individual’s data. These include relevant privacy notices that are published online at Sutton Mencap and distributed to staff and volunteers.

This policy explains how Sutton Mencap will hold and process your information. It explains the rights of data subjects. It also explains the obligations of staff and volunteers when obtaining, handling, processing or storing personal data in the course of working for, or on behalf of, Sutton Mencap.

This policy does not form part of a contract of employment (or contract for services if relevant) and can be amended by Sutton Mencap at any time.

**Scope of the policy**

This policy applies to all individuals for whom personal data is processed by Sutton Mencap, including staff, volunteers, trustees, service users, carers, supporters, members and donors. It applies to people who currently have a relationship with Sutton Mencap and those who previously had a relationship, such as ex-staff or previous service users. Individuals that fall into one of these categories are defined as a ‘data subject’ for the purposes of this policy.

It covers the collection, maintenance, use and destruction of personal data, the collection, maintenance, use and destruction of employment records (including for previous staff and volunteers), processes for sharing, information and individual’s access to information.

**Data Protection Principles**

Personal data must be processed in accordance with six ‘**Data Protection Principles**.’ It must:

* be processed fairly, lawfully and transparently;
* be collected and processed only for specified, explicit and legitimate purposes;
* be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
* be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;
* not be kept for longer than is necessary for the purposes for which it is processed; and
* be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

**How we define personal data**

‘**Personal data**’ means information which relates to a living person who can be **identified** from that data (a ‘**data subject**’) on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

This personal data might be provided to us by the individual concerned. It could also be provided by someone else. For examples in the case of a staff member, this could be a former employer, a doctor, the Disclosure and Barring Service, or a credit reference agency. For a service user, it might be a referral from another agency.

Personal data could also be created by us. It could be provided or created during the recruitment process or during the course of a contract of employment/ services or after its termination. It could be created by a manager or other colleagues.

The types of personal data we collect and use about individuals is included in the relevant Privacy Notice. For staff, this is issued with a contract of employment. Privacy notices for other individuals are also posted online.

**How we define special categories of personal data**

‘**Special categories of personal data**’ are types of personal data consisting of information as to an individual’s:

* racial or ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* genetic or biometric data;
* health;
* sex life and sexual orientation; and
* any criminal convictions and offences.

We may hold and use any of these special categories of personal data, as detailed in the Privacy Notice, in accordance with the law.

**How we define processing**

**‘Processing’** means any operation which is performed on personal data such as:

* collection, recording, organisation, structuring or storage;
* adaption or alteration;
* retrieval, consultation or use;
* disclosure by transmission, dissemination or otherwise making available;
* alignment or combination; and
* restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

**How will we process personal data**

Sutton Mencap will process an individual’s personal data (including special categories of personal data). We will use personal data for:

* performing the contract of employment (or services) between us;
* complying with any legal obligation; or
* if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if the individual’s interests and rights do not override ours or a third-party’s. An individual has the right to challenge our legitimate interests and request that we stop this processing.

We can process personal data for these purposes without the knowledge or consent of the individual. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

Examples of when we might process an individual’s personal data can be found in the relevant Privacy Notice. We will only process special categories of personal data in certain situations in accordance with the law. For example, we can do so if we have an individual’s explicit consent. If we asked for consent to process a special category of personal data then we would explain the reasons for our request. An individual does not need to consent and can withdraw consent later if they choose by contacting the Office Manager, who is the person responsible for data at Sutton Mencap.

We do not need your consent to process **special categories** of your personal data when we are processing it for the following purposes, which we may do:

* where it is necessary for carrying out rights and obligations under employment law;
* where it is necessary to protect an individual’s vital interests or those of another person, where either are physically or legally incapable of giving consent;
* where an individual has made the data public;
* where processing is necessary for the establishment, exercise or defence of legal claims;
* where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.
* where processing is necessary to deliver an appropriate service which meets individual needs.
* Where processing is necessary in relation to working with children or vulnerable adults, e.g. criminal convictions and information identified via the Disclosure and Barring Service.

We might process special categories of personal data for the purposes stated in the Privacy Notice, in particular, we may use information in relation to:

* race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities;
* sickness absence, health and medical conditions to monitor absence, assess fitness for work, to pay benefits, or to comply with our legal obligations under employment law including to make reasonable adjustments and to look after an individual’s health and safety; and

We do not take automated decisions about any individual using their personal data or use profiling in relation to any individual.

**Sharing personal data**

Sometimes we might share personal data with other agencies to carry out our obligations under our contract with an individual or for our legitimate interests.

We require those companies to keep personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process data for the lawful purpose for which it has been shared and in accordance with our instructions.

We use the following contractors to carry out our business:

All individuals

* Co-op systems. ICT support provider. Support includes moving data between devices, and disposal of old ICT equipment.

Staff and volunteers:

* The HR Dept. Provide advice on managing HR issues, including support and advice with individual employees.
* My HR Toolkit: to process HR information.
* Sage: accounting information, eg in relation to payment of expenses.
* CAFBank: banking services to make payments to staff.
* Brightpay: Payroll services
* FindMyShift: to record timesheet data, including annual leave, sickness and other absence.

Service users, carers and supporters:

* Charitylog online database, to record contact information, membership of specific services, attendance at services (adults) for providing invoicing information.
* FindMyShift: Attendance at services (children and young people), for providing invoicing information.

These contractors have confirmed to us that their normal (regular) data processing activities all occur within the European Union/ European Economic Area, with all databases, servers, and backups located in EU/EEA data centres. They have also confirmed that data will not be transferred outside this area, unless the third country has been deemed by the EU Commission to ensure an appropriate level of protection, the recipient of the data guarantees an acceptable level of data protection in accordance with EU standard contractual clauses for the transmission of personal data, or there are other safeguards in place that permit such a transfer.

**How employees should process personal data for Sutton Mencap**

Everyone who works for, or on behalf of, Sutton Mencap has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and our Information and Community Technology policy.

Sutton Mencap’s Director, supported by the Office Manager, is responsible for reviewing this policy on our data protection responsibilities and any risks in relation to the processing of data. Staff should direct any questions in relation to this policy or data protection to either person.

Staff must only access personal data covered by this policy if they need it for the work they do for or on behalf of Sutton Mencap and only if they are authorised to do so. Staff must only use the data for the specified lawful purpose for which it was obtained. Any doubts regarding accessing or using data should be addressed to their line manager, the Office Manager of the Director.

Key instructions for staff and volunteers are as follows:

* Do not share personal data informally
* Keep personal data secure and not share it with unauthorised people.
* Regularly review and update personal data which you have to deal with for work. This includes telling the Office Manager if your own contact details change.
* Do not make unnecessary copies of personal data and should keep and dispose of any copies securely.
* Use strong passwords.
* Lock computer screens when not at the desk.
* Consider anonymising data or using separate keys/ codes so that the data subject cannot be identified.
* Do not save personal data to your own personal computers or other devices.
* Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Director.
* Lock drawers and filing cabinets. Do not leave paper with personal data lying about. Pay particular attention to the printer/ photocopier.
* Do not take personal data away from Sutton Mencap’s premises without authorisation from your line manager. Files containing personal data must be returned to Sutton Mencap after use.
* Personal data should be shredded and disposed of securely when you have finished with it.
* Ask for help from your line manager, the Office Manager or the Director if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

Any deliberate or negligent breach of this policy by a staff member may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

**How to deal with data breaches**

Sutton Mencap has robust measures in place to minimise and prevent data breaches from taking place. Should a breach of any personal data occur it must be reported and we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals, then we must also notify the Information Commissioner’s Office within 72 hours.

If you are aware of a data breach you must contact the Director immediately and keep any evidence you have in relation to the breach.

**Subject Access request**

Data subjects can make a ‘**subject access request**’ (‘SAR’) to find out the information we hold about them. Details on how we respond to an SAR is set out in the Subject Access Request procedure.

If a staff member receives such a request, it must be forwarded immediately to the Office Manager who will coordinate a response. If a staff member would like to make a SAR in relation to their own personal data, it should be made in writing to the Office Manager. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

There is no fee for making a SAR. However, if a request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to the request.

**Data retention**

Our normal data retention periods are as follows:

Staff records (based on guidance from the HR department, 2016):

* Contents of employee files to be kept for 6 years following staff member leaving.
* After 6 years, we will keep a record of the staff name and date of birth for identification purposes, plus start and finish dates. This is for the purpose of responding to reference requests.
* As required, we will keep health and sickness records, accident and incident reports and any health and safety records for a period of 40 years, after which they will be destroyed.
* We will keep parental leave records for 18 years,

Records in relation to adult clients and their parent/ carers (based on guidance from the Information governance alliance, 2016):

* All records will normally be kept for 8 years from the date of ceasing to use our service.
* After 8 years we will keep a record of the service user’s name and date of birth for identification, plus start and end dates of service use.
* We will keep records of non-serious incidents for 10 years from the date of the incident.
* We will keep records any serious incidents for 20 years from the date of the incident.

Records in relation to children and young people and their parent/ carers (based on guidance from the Information governance alliance, 2016):

* All records will normally be kept until their 25th birthday (26th birthday if they are still accessing a service from us at the age of 17).
* After their 25th or 26th birthday, we will keep a record of the service user’s name and date of birth for identification, plus start and end dates of service use.
* We will keep records of non-serious incidents for 10 years from the date of the incident.
* We will keep records any serious incidents for 20 years from the date of the incident.

These are normal intended retention periods. Individuals can still exercise their right to request that personal data is erased before the retention period ends (see rights of data subjects below).

**The rights of data subjects**

All individuals have the right to information about what personal data we process, how and on what basis as set out in this policy. Individuals can exercise these rights by contacting Sutton Mencap’s Office Manager.

Individuals have the following rights:

* to access their own personal data by way of a subject access request (see above).
* To request that we correct any inaccuracies in their personal data.
* To request that we erase personal data where we are not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected.
* to apply for the use of personal data to restricted, including whilst a request to correct or erase personal data is being considered.
* to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.
* to object if we process your personal data for the purposes of direct marketing, even if you have previously given consent for this.
* to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month
* not to be subjected to automated decision-making.
* to be notified of a data security breach concerning your personal data.

In most situations we will not rely on an individual’s consent as a lawful ground to process your data. If we do however request consent to the processing of personal data for a specific purpose, an individual has the right not to consent or to withdraw your consent later. This can be done by contacting the Office Manager.

Individuals also have the right to complain to the Information Commissioner, by contacting the Information Commissioner’s Office directly. Full contact details including a helpline number can be found on the Information Commissioner’s Office website ([www.ico.org.uk](http://www.ico.org.uk)). This website has further information on individual’s rights and our obligations.

**Related policies**

* Subject Access Request procedure
* Sutton Mencap privacy notices
* Recruitment and selection policy
* Confidentiality policy
* Information and Communication Technology policy

**Responsibilities**

**Trustees**

* To approve and review the policy on a regular basis
* To take reasonable steps to satisfy themselves that the policy is being implemented.

**Senior staff**

* To act in accordance with the policy and related procedures.
* To communicate the policy to other staff and volunteers and to ensure it is being implemented correctly.

**All Staff and volunteers**

* To act in accordance with the policy and related procedures

**Signed on behalf of the Trustee Board of Sutton Mencap**

**Chairman: Date: June 2018**

 **Mavis Peart**

**Next review: June 2021**