****

**Information and Communication**

**Technology policy**

**Aims**

* To ensure Sutton Mencap is able to maximise the benefits from Information and Communication Technology (ICT) on behalf of service users, carers and the organisation.
* To ensure the use of ICT promotes the safeguarding of service users, staff and volunteers.
* To ensure Sutton Mencap complies with its legal responsibilities in relation to the use of ICT.
* To project Sutton Mencap’s reputation.
* To protect the ICT resources that Sutton Mencap has invested in.

**Introduction**

Sutton Mencap recognises that the use of information and communication technology can play an increasingly important role in supporting the delivery of high quality services. This policy sets out how access to equipment, facilities and information by staff, volunteers and service users will be managed. All employees are encouraged to make appropriate use of the opportunities presented by the medium but failure to abide by this policy will be regarded as serious misconduct.

This policy must be read in alongside Sutton Mencap’s Data Protection Policy to ensure that there is a full understanding of the organisation’s responsibility with regard to data.

**Scope**

This policy applies to all staff and volunteers. It also applies to any service users, carers and visitors who make use of Sutton Mencap ICT equipment or facilities.

**Use of Sutton Mencap equipment**

* Equipment should be used appropriately in accordance with Sutton Mencap’s Health and Safety Policy.
* Sutton Mencap may check and review an individual’s computer files and internet and IT usage at Sutton Mencap.

**Software**

* Staff and volunteers are only authorised to use the packages provided on the system.
* Installation of any additional software requires the permission of the Director.
* Use of software must be in in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges, as well as disciplinary action.

**Keeping the system secure**

* Where required, staff/ volunteers will be issued with passwords to enable access to Sutton Mencap’s ICT systems. Staff and volunteers must keep their log in information safe and should only use their own log in.
* Staff/ volunteers should contact the Office Manager if they believe their password is no longer secure.
* Information about people must be recorded and obtained in accordance with Data Protection legislation and Sutton Mencap’s Data Protection Policy.
* Staff/volunteers should not attempt to gain unauthorised access to information or facilities on Sutton Mencap’s ICT systems. If staff/ volunteers feel they are unable to access information or facilities they need, they should raise this with their line manager.
* Unless they are automatically scanned by a server, files or programmes accessed from outside Sutton Mencap’s ICT system, including from memory sticks, flash drives, portable hard drives, CD-ROM, internet and e-mail attachments must be scanned for viruses before they are opened or copied onto Sutton Mencap’s system.
* Particular care should be taken with e-mail attachments. If there is any doubt about the origin of an e-mail, delete the e-mail without opening the attachment.
* A back up of the server will take place during office hours. Back up cartridges will be taken off site.
* Data should be stored on the server and not on individual computers (e.g. the C: Drive), to ensure it is included in the back up.

**Use of Sutton Mencap devices outside of the office**

* Sutton Mencap may make devices such as laptop computers and tablets available for staff to use outside of the office as part of their work.
* Staff should ensure that any Sutton Mencap log in details are not saved on the device. This includes remote access to e-mails, server and any cloud-based systems such as a database.
* Staff should take care in the transporting and use of the device in public places and avoiding putting themselves at any risk.
* The Office Manager should be informed that the device is being taken out of the premises.
* Loss or theft of the device must be reported immediately.
* Staff should take care when accessing wi-fi outside of Sutton Mencap and should seek to verify the authenticity of any wi-fi system used.

**Use of own devices**

Sutton Mencap staff and volunteers are not required to use their own devices for business purposes. Sutton Mencap may allow staff and volunteers to use their own equipment, such as smart phones, tablets, laptops and home computers in connection with Sutton Mencap business, provided that the following procedures are adhered to:

* Staff must get prior permission from their line manager or the Director to use their own devices to access Sutton Mencap’s server, e-mail system or database.
* The device must be used in accordance with this policy. Failure to do so may result in Sutton Mencap revoking the right to use the personal device.
* The device must lock itself with a Personal Identification Number (PIN) set by the staff member. Your device should automatically lock itself after a maximum time out period of 5 minutes.
* Staff should take care when accessing wi-fi outside of Sutton Mencap and should seek to verify the authenticity of any wi-fi system used.
* Loss or theft of the device must be reported immediately to a line manager or office manager.
* Expenses such as carrier costs or hardware will not be reimbursed by Sutton Mencap unless agreed in advance with the Director.

**Personal use of Sutton Mencap equipment**

Personal use of Sutton Mencap equipment outside of work time for a reasonable and specific purpose is allowed, so long as it does not:

* Incur specific expenditure for Sutton Mencap;
* Interfere with the employees’ work;
* Break the law, or bring Sutton Mencap into disrepute. Employees must not view material that is sexually explicit or obscene or would be considered offensive or harassing to individuals / groups of individuals.

**Use of the internet**

* Sutton Mencap encourages staff and volunteers to make use of the World Wide Web as a tool or resource to support their normal duties and responsibilities.
* Staff/ volunteers will not use electronic communication facilities provided by Sutton Mencap to deliberately access, view or download any material in whatever format or medium that is pornographic, abusive, offensive, defamatory or discriminatory or that would constitute in any way an action contrary to UK or International law or Sutton Mencap policy.
* Sutton Mencap recognises the possibility that an employee/ volunteer may, inadvertently, access material that would constitute a breach of this policy. They must immediately report the incident to their line manager.
* Sutton Mencap reserves the right at any time to check web sites visited and material downloaded.
* Staff must not use the internet to transmit confidential personal or business sensitive information, without the data being protected.

**Use of e-mail**

* Email is a fast and effective means of communicating both internally and externally and should be used when appropriate for the purpose.
* Where required, staff/ volunteers will be allocated an e-mail account with a personalised address for work-related communications.
* The Director will determine when, and in what circumstances, additional e-mail accounts/addresses are to be created and to which member(s) of staff they will be assigned.
* Staff are responsible for the proper maintenance of all e-mail accounts that are assigned for their use. This responsibility includes:
  + Ensuring that e-mail accounts are checked periodically and new messages downloaded.
  + Responding to e-mail messages where such messages fall within their normal duties and responsibilities.
  + Forwarding e-mail messages that fall outside their normal duties and responsibilities to an appropriate other member of staff.
  + Archiving or deleting e-mail messages that are no longer in use.
  + Filing important documents.
* Email should be used responsibly for legitimate work related purposes. When using email the normal standards of courtesy and professionalism associated with other forms of written and spoken communication should be adhered to.
* Employees must not send or knowingly send or save material that is sexually explicit or obscene or would be considered offensive or harassing to individuals / groups of individuals.
* Employees should also not send defamatory, abusive, intimidating or discriminatory messages.
* Employees should not send any message that may breach the intellectual property rights of an individual or body corporate.
* Any email sent or received via a Sutton Mencap email addresses is open to examination by the Director.

**Use of Sutton Mencap facilities by people who are not employed, including service users**

* Sutton Mencap recognises the value of the use of ICT equipment by service users, carers and other visitors to the building.
* Any access to wi-fi by service users, carers and other visitors will be via a designated public system and not via Sutton Mencap’s private wi-fi system.
* Use of Sutton Mencap ICT equipment will be in accordance with this policy.

**Personal use of social networking**

* All staff and volunteers should be aware that the internet is not a private or confidential system and that Sutton Mencap has a legitimate interest in protecting the charity, its staff and service users from abuse or harm to reputation resulting from information on the internet.
* Staff who publish details of their employment/ volunteering with Sutton Mencap, or where it can be reasonably worked out that the staff are employed by/ volunteer for Sutton Mencap, should be aware that they are responsible for these details.
* Staff who make reference to their employment/ volunteering with Sutton Mencap must use the following disclaimer: “The views contained in these web pages are my personal views and do not represent the views of Sutton Mencap.” Staff should note, however, that this disclaimer does not exonerate them from their responsibility to adhere to all statements and rules in this policy.
* Staff should regard all information posted on the internet as being available to the public. This includes text and photographs. In this respect, staff should have no expectation of privacy in relation to information on the internet. This charity does not recognise any “privacy setting” which renders any postings unreadable or restricted.
* Staff must avoid posting any content on the internet which may bring the charity into disrepute. Staff are prohibited from using copyrighted materials, unfounded or derogatory statements, misrepresented material and should not name anyone in relation to Sutton Mencap.
* Staff should not reveal any information that could be considered confidential to Sutton Mencap, a colleague or service user and their family.
* Staff receiving any press or media contact in relation to the information they have posted on the internet about Sutton Mencap must advise the Director.
* It is recognised that staff members who commonly use social media may encounter service users or their carers using the same media. Staff should not actively seek out service users or their carers on social media.
* If service users or carers make contact with staff members on social media, staff should discourage said contact. Staff members should not “friend” services users or carers or contact them directly through social media. If a service user or carer makes contact with a staff member, that staff member should advise their line manager immediately.
* If staff members are in contact with service users or carers as a result of a relationship outside of Sutton Mencap (family, family friends, etc) which makes contact through social media appropriate, the staff members should advise their line manager.
* If in contact with service users or carers via social media, staff should conduct themselves according to Sutton Mencap’s code of conduct, even if such contact takes place outside of working hours.
* If in any doubt, staff should contact their line manager or the Director.

**Related policies**

* Data protection policy
* Code of conduct
* Confidentiality policy
* Health and Safety policy
* Professional Boundaries policy
* Safeguarding 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.
* To communicate the policy to other staff and volunteers and to ensure it is being implemented correctly.
* To advise staff on any issues or concerns that arise with the implementation of the policy
* To monitor performance of the policy and report to trustees

All Staff and volunteers

* To act in accordance with the policy
* If in doubt, to raise any issues or queries in relation to the policy with a line manager or the Director.

**Signed on behalf of the executive committee of Sutton Mencap**

**Chairman:  Date: June 2018**

**Mavis Peart**

**Review: June 2021**