Southend Mencap Data Protection and Information Collecting Policy

The Data Protection Act 2018 is a UK law that updates data protection laws in the UK, complementing the General Data Protection Regulation (GDPR) and implementing the EU Law Enforcement Directive. It gives individuals more control over their personal data and provides organisations with guidance on how to process data lawfully.

The Data Protection Act 2018 requires every data controller who is processing personal data to notify unless they are exempt. Failure to notify is a criminal offence. Southend Mencap has a direct debit in place to renew our notification each year for the following purposes:

- Staff administration
- Advertising, marketing and public relations
- Accounts and records
- Administration of membership records
- Advertising, marketing and public relations for others
- Advocacy and information support
- Fundraising
- Information and databank administration
- Journalism and media
- Realising the objectives of a charitable organisation
- Trading/sharing in personal information

IF Southend Mencap needs to collect data for any purpose not stated above we should notify the Information Commissioner before collecting that data.

Eight Data Protection Principles

Whenever collecting information about people, Southend Mencap agrees to apply the Eight Data Protection Principles:

1. Personal data should be processed fairly and lawfully
2. Personal data should be obtained only for the purpose specified
3. Data should be adequate, relevant and not excessive for the purposes required

4. Accurate and kept up-to-date
5. Data should not be kept for longer than is necessary for purpose
6. Data processed in accordance with the rights of data subjects under this act
7. Security: appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to personal data.
8. Personal data shall not be transferred outside the EEA unless that country or territory ensures an adequate level of data protection.

Notes for Southend Mencap*:*

- The data controller must provide their identity, people should be told exactly what the information is being collected for and any other information necessary. We must get their consent.
- We should think in advance about what we wish to do with personal data, i.e. if we get names and addresses for a specific campaign we should only use that info for that campaign
- Individuals have a right to see what data is being kept on them, and for what purpose, which we will provide within 20 days of the request.
- Same principals need to apply when data is taken out of the office.
- If we buy in a mailing list we cannot use it for any other purpose than the original Data Controller specified – we must check original use.
- Clients have the right to have their personal data deleted from Southend Mencap's files. If this is the case, clients need to confirm this in writing with specific mention of the Oasis and CADS systems the society holds personal client data on.

Working from home

- Southend Mencap keeps note of which staff takes work home with them.
- If working on something at home and at work, only the one file should be used i.e. begin at work, copy and take home, work on at home, then copy and update back at work.
- Home computers should have records removed once project/work records no longer needed at home.
- Staff agree to keep work taken home very secure, to only keep work at home when it is being actively worked on and Southend Mencap must be informed if any information has got into wrong hands.

Special funding tracking requirements and data protection

- Try not to keep more than project/tracking requires
- The more information kept the more secure it should be kept
- If publishing staff/volunteers/students' details, tell them
- Take extra care if records include sensitive data
- Only keep personal data as long as necessary under funding rules
- Don't keep surplus information.

Security Statement

Southend Mencap has taken measures to guard against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage.

This includes:

- Adopting an information security policy (this document is our policy)
- Taking steps to control physical security (projects and staff records are all kept in a locked filing cabinet)
- Putting in place controls on access to information (***password protection on files and server access***)
- Establishing a business continuity/disaster recovery plan (Southend Mencap takes regular back-ups of its computer data files and this is stored in a locked filing cabinet)
- Training all staff on security systems and procedures
- Detecting and investigating breaches of security should they occur