St Albans Mencap

Charity number: 210073

stalbansmencap.org.uk

Data Protection Policy

This document outlines the Data Protection Policy of St. Albans Mencap, it aims to provide a concise and practical document that can be used by trustees, staff and volunteers to understand their responsibilities under UK GDPR and in how they collect and handle information about people with whom they work.

Document control:

Version:	Date approved:	By:	Review due:
0.1	Dec 2025	Board of Trustees	Dec 2026

Summary of changes:

Version:	Changes:
0.1	Re-draft of existing 2019 policy

Definitions

Charity	means St Albans Mencap, a registered charity.
GDPR	means the General Data Protection Regulation.
Responsible Person	means [TBC name of person responsible for data protection within the Charity].
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Charity.

1. Data protection principles

The Charity is committed to processing data in accordance with its responsibilities under the GDPR.
Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. 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."

2. General provisions

a. This policy applies to all personal data processed by the Charity.
b. The Responsible Person shall take responsibility for the Charity's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Charity shall register and maintain its registration with the Information Commissioner's Office as an organisation that processes personal data (see Annex 1 - SAM ICO Data Protection Registration Details and Certificate).

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems (see Annex 2 – SAM Register of Systems).
b. The Register of Systems shall be reviewed at least annually as part of this policies review.
c. Individuals have the right to access their personal data and any such requests made to the charity shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the charity must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Charity shall note the appropriate lawful basis in its Register of Systems (see Annex 2 – Register of Systems).
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Charity's systems.

5. Data minimisation

a. The Charity shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Charity shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Charity shall put in place an archiving policy for each area in which personal data is processed and review this process annually as part of this policies annual review.
b. The archiving policy shall consider what data should/must be retained, for how long, and why.

8. Security

a. The Charity shall ensure that personal data is stored securely using modern software that (version, patches, etc) is kept-up-to-date.
b. Access to personal data shall be limited to personnel (trustees, staff, volunteers, etc.) who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

9. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Charity shall promptly

assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (reporting breach information on the ICO website).

The charity will ensure that is has untaken preparation in advance ahead of any data breach occurring.

'Annex 3 - Preparing in advance to deal with a data breach' details actions that should be undertaken as part of these advance preparations.

Annex 1 – SAM ICO Data Protection Registration Details and Certificate

Registration reference: ZA822550
Date registered: 23 August 2022
Registration expires: 22 August 2026
Payment tier: Tier 1
Data controller: St Albans Mencap Limited
Address: 103 Stanley Avenue, Chiswell Green, St. Albans, AL2 3AQ

Data Protection
Registration Certificate

St Albans Mencap Limited

103 Stanley Avenue
Chiswell Green,
St. Albans
AL2 3AQ

Registration reference: ZA822550
Date registered: 23 August 2022
Registration expires: 22 August 2026

Issued by: Information Commissioner's Office,
Wycliffe House, Water Lane, Wilmslow, Cheshire
SK9 5AF

Telephone: 0303 123 1113
Website: ico.org.uk

Annex 2 – Register of Systems

The register of systems table below aims to:

1. Identify all data handling systems currently in use within your organization.
2. Document the purpose and functionality of each system.
3. Record the data types each system protects and their compliance requirements.
4. Include details on system owners and responsible personnel for each system.
5. Establish a review schedule to keep the register updated and accurate.

By keeping the table up to date with respect to all of SAM's systems currently holding data the register aims to ensure that the data held by SAM is understood by trustees, staff and volunteers and therefore the data held in the systems is transparent and accountable in how it is held and used within SAM for relevant stakeholders.

Register of Data Protection Systems

SAM Data Protection System /System Holding Personal Data	Purpose and Functionality of the System	Data Held on system and Compliance Requirements	System Owner / Responsible Person for System

Annex 3 – Preparing in advance to deal with a data breach

There are lots of small ways data can accidentally be breached, or be put at risk of a breach. For instance:

- someone can accidentally cc an email that should have been bcc'd (addresses hidden)
- someone tries to do something good by sharing data but hasn't checked permissions and consent for this new use
- out-of-date software can 'leak data' meaning it sends data around the internet or offices and file systems in ways that aren't considered secure any more
- the wrong link can be sent to the wrong person
- a service you use can change its terms and conditions and take data without you noticing
- malware has got into your systems
- someone has been the victim of a phishing attack.

To lower your risks:

- check and update systems regularly
- make sure all staff and volunteers know not to share data
- make sure all staff and volunteers know how to report a breach (however minor the risk)
- train your staff regularly on data protection
- be clear that the organisation needs to know what has happened as quickly as possible so it can take actions and learn.

Get ready for things going wrong by having procedures or steps to follow.

- Decide when you need to let the people who could be affected know and how you will do this.
- Check whether the breach meets the rules that mean you must report it to the ICO within 72 hours of being made aware of it.
- Include the ICO small organisation helpline in your procedures to help you (0303 123 1113).
- Update your data processing procedures to reduce the risk of it happening again.
- Develop training to reduce future risks.

Organisations holding more sensitive data need additional measures.

- Reduce the likelihood of some types of breach by following these five first steps to cybersecurity: 1) Backing up your data; 2) Protecting the charity from Malware; 3) Keeping your smartphones (and tablets) safe; 4) Using appropriate passwords to protect your data; and 5) Avoid phishing attacks
- Use the ICO's advice on preparing to deal with a personal data breach.