

St Albans Mencap

Charity number: 210073

stalbansmencap.org.uk

Online Safety Policy

St Albans Mencap is committed to protecting children, young people, and vulnerable adults from online harm by promoting safe and responsible use of digital technologies across all its services.

Document control:

Version:	Date approved:	By:	Review due:
1.0			

Summary of changes:

Version:	Changes:
1.0	Redrafted in current format – July 2025

Online Safety Policy Statement

Purpose and Scope

St Albans Mencap is committed to safeguarding and promoting the welfare of children, young people, and vulnerable adults who access our services. This Online Safety Policy Statement outlines our approach to ensuring that all individuals involved in our activities are protected from online harm and that digital technologies are used safely and responsibly.

This policy applies to all staff, trustees, volunteers, agency workers, and students working on behalf of St Albans Mencap, as well as to children, young people, and families who engage with our services.

Our Commitment

- Ensuring the safety and wellbeing of children, young people, and vulnerable adults when using the internet, social media, and digital devices.
- Supporting children and young people to use the internet for education, communication, and personal development in a safe and informed way.
- Providing clear guidance to staff and volunteers on acceptable use of digital technologies and online conduct.
- Embedding online safety into our safeguarding, training, and service delivery practices.

Key Principles

- The welfare of the child or vulnerable adult is paramount.
- All individuals have the right to equal protection from all types of online harm or abuse.
- Online safety is a shared responsibility between the organisation, staff, volunteers, children, young people, and their families.

Online Safety Measures

- All staff and volunteers will receive training on online safety and acceptable use of digital platforms.
- Children and young people will be supported to understand online risks and how to protect themselves.
- Any concerns about online behaviour or content will be reported and managed in line with our safeguarding procedures.
- Devices used during activities will be monitored and protected with appropriate filters and security settings.

Acceptable Use

- Staff and volunteers must not engage in private online communication with children or young people outside of agreed platforms and times.
- Children and young people will be asked to sign an Online Safety Agreement outlining expected behaviour when using digital tools during Mencap activities.

Social Media Guidelines

- Staff and volunteers must not post images or personal information about children, young people, or vulnerable adults on personal social media accounts.
- Official social media accounts must be managed by authorised personnel and used in accordance with our communications and safeguarding policies.
- Consent must be obtained from parents/carers before sharing any photos or stories involving children or vulnerable adults.
- Any online harassment, bullying, or inappropriate content involving our community must be reported to the Designated Safeguarding Lead (DSL) immediately.
- Staff and volunteers must not accept friend or follow requests from service users on personal accounts.

Staff Training Requirements

All staff, trustees, and volunteers must complete mandatory online safety training as part of their induction. Refresher training will be provided annually or in response to significant changes in legislation, policy, or technology.

Training will cover:

- Recognising online risks and signs of harm.
- Safe use of digital tools and platforms in service delivery.
- Procedures for reporting and responding to online safety concerns.
- Responsibilities under the Data Protection Act and safeguarding legislation.

The Designated Safeguarding Lead will maintain a training log and ensure compliance across the organisation.

Data Protection Compliance

- All personal data collected, stored, or shared through digital platforms must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.
- Staff and volunteers must only access personal data necessary for their role and must handle it securely and confidentially.
- Digital records must be stored on secure systems with appropriate access controls and encryption where necessary.
- Personal data must not be shared via unsecured channels such as personal email or messaging apps.
- Any data breaches or suspected breaches must be reported immediately to the Data Protection Officer or DSL and will be managed in line with our Data Protection Policy and breach response procedures.

Reporting and Response

All online safety concerns will be recorded and referred to the DSL or Deputy DSL. Serious incidents will be escalated to the Operations and Safeguarding Committee and, where necessary, to external safeguarding authorities.

St Albans Mencap Online Safety Policy

Review and Compliance

This policy will be reviewed annually or in response to changes in legislation, NSPCC guidance, or organisational practice. It aligns with the NSPCC's safeguarding principles and is supported by our broader safeguarding, data protection, and anti-bullying policies.