

Data Protection Policy and Privacy Notice

SEND Empowerment Advocacy

2026

Effective date 10/10/26 | Review date 10/10/27

This policy explains how we handle personal information when people enquire about or use our free SEND advocacy service, register for events or receive updates. It also sets the standards that our team must follow to protect children, young people and families. It applies to digital and paper records and to everyone handling information on our behalf.

1 Who is responsible for your information

SEND Empowerment Advocacy decides why and how personal information is used for its service and is the data controller.

Data Protection Lead: Marnie Harvey. Email: marnieh@send-empowerment.co.uk. Website: <https://www.send-empowerment.co.uk>. Contact us to ask about this policy, withdraw consent, exercise your rights or make a data protection complaint.

We follow the UK GDPR, the Data Protection Act 2018 and applicable Privacy and Electronic Communications Regulations, as amended. We process information lawfully, fairly and transparently, for clear purposes, using only what is necessary. We keep it accurate, protect it and retain it only as long as justified.

2 Information we collect and where it comes from

We may collect your name, email address, telephone number, local authority, relationship to the child or young person, parental responsibility or other authority to act, support requested and relevant information about other services involved. We collect a date of birth, address or other identifying detail only where needed for a particular task.

Casework information may include a child or young person's details, educational needs, school attendance, EHCPs, assessment reports, diagnoses, health and disability information, family circumstances, correspondence, meeting notes, advice and outcomes. Health information and some other information are special category personal data and require additional protection.

We obtain information directly from you through forms, email, telephone calls, meetings and documents you provide. With appropriate authority, we may receive relevant information from schools, local authorities, professionals or other services. We explain this use to the person concerned, or their appropriate representative, within the legally required period unless an applicable exemption permits otherwise.

Event registration may include contact details, chosen sessions and accessibility requests. Newsletter records include contact details and subscription preferences. Our website providers may also process technical information such as IP addresses, logs and cookie preferences, as explained in section 11.

Please provide only information relevant to your request. Do not send unnecessary details about other people. We assess our own lawful basis and any additional condition for information about each person; your permission does not automatically authorise all processing of another person's data.

3 How and why we use information

We use relevant information to respond to enquiries, create and maintain contact records and support tickets, assess the support requested, allocate suitable team members and communicate with you. We also use it to prepare advocacy documents, support casework and keep an accurate record of advice and actions.

We may use necessary information to manage complaints, maintain security, address safeguarding concerns, meet specific legal requirements and evaluate service quality. Internal supervision and quality checks are limited to authorised team members who need access.

We use anonymised statistics to understand demand, outcomes and barriers in the SEND system and to support service development and reporting. Creating those statistics from personal information is itself processing and requires a lawful basis and, where applicable, an Article 9 condition. Removing names alone does not make information anonymous; we check that individuals cannot reasonably be identified, including from combinations of details. Identifiable case studies or testimonials require separate, specific permission.

4 Our lawful bases

We identify and record the lawful basis before processing. Accepting terms or acknowledging this notice is not consent to every use of information. The following describes the proposed approach for our service; it must be approved against our actual activities before implementation.

Enquiry administration, contact records, support tickets and ordinary casework: Article 6(1)(f), legitimate interests in operating a free advocacy service, responding to requests and maintaining necessary records. We document why processing is necessary and balance our interests against the person's rights, giving particular weight to children's interests. If that assessment does not support the processing, we do not use this basis.

Relevant health and disability information for requested advocacy: Article 6(1)(f), where the above assessment supports it, together with Article 9(2)(a), explicit consent. Consent must identify the information and purpose, be freely given, specific and informed, and be recorded. We do not assume that offering SEND advocacy makes us a regulated health or social care provider.

Optional newsletters, general event invitations and promotional updates: Article 6(1)(a), consent, with any consent required under PECR. Requested event booking confirmations, joining instructions and resources are service communications; ordinary contact details may be processed under legitimate interests for delivering the requested event. Health or accessibility information requires a separately identified Article 9 condition, normally explicit consent.

Complaints, security and service oversight: legitimate interests, subject to assessment. If special category information is necessary, we separately establish and record a valid Article 9 condition. Consent for advocacy does not automatically cover unrelated research or other new purposes.

Legal obligations: Article 6(1)(c) only where a specific legal duty applies; we record that duty. Legal claims: an appropriate Article 6 basis and Article 9(2)(f) where special category information is necessary for establishing, exercising or defending legal claims. This does not justify routinely retaining every case file.

Safeguarding: we identify the basis for the actual circumstances, which may include legitimate interests, a relevant recognised legitimate interest or a specific legal obligation. For special category information, Article 9(2)(g) and Schedule 1 paragraph 18 of the Data Protection Act 2018 may apply only where all conditions for safeguarding children or individuals at risk are met. We put an appropriate policy document in place where

required. Vital interests is used only where its legal requirements are satisfied; the special category condition requires that the person is physically or legally incapable of giving consent.

Criminal allegation, offence or conviction information is governed by separate Article 10 rules. We do not process it merely because it appears in a referral; we first identify an applicable legal authorisation and any required safeguards.

5 Consent and information about children

A separate unticked checkbox or other clear statement is used for explicit consent to relevant health and disability information. We retain the wording and policy version, date, method, identity of the person consenting and what they agreed to. Marketing, external casework contact and disclosure to event hosts are separate choices.

You can withdraw consent at any time by contacting us. This does not affect processing that was lawful before withdrawal. We stop the relevant consent-based processing, unless a separate lawful reason requires particular information to be kept or used, which we explain. We do not retrospectively change the lawful basis simply to avoid respecting withdrawal.

You can make an initial enquiry without sharing health information. If you decline or withdraw consent to information necessary for personalised advocacy, we explain what support remains possible and what we cannot provide without it. Optional marketing and unrelated disclosures are never a condition of receiving support.

A child's information belongs to the child. We consider their understanding and ability to make decisions, parental responsibility and any other valid authority to act. We do not assume that a parent can consent for a competent young person or an adult child. We involve children and young people appropriately and explain privacy information in an accessible way.

6 Who can access information and when we share it

Authorised administrators, advisers, EHCNA writers, supervisors and the Lead Advocate access only the information necessary for their assigned role. Volunteers are subject to confidentiality and data protection requirements.

For routine casework, we obtain specific authority before contacting a school, local authority, healthcare professional or another organisation on your behalf. We record who we may contact, the purpose and scope of information sharing. A website enquiry or acceptance of this policy does not grant general permission to contact external organisations.

We may disclose necessary information without permission where an applicable law requires it or a lawful safeguarding disclosure is justified. We document the reason, recipient and information disclosed, and tell you where lawful and safe to do so.

Technology providers supporting our website, email, ticketing, contact management, document storage and online meetings may process information on our behalf under appropriate contracts.

For events, we explain in advance whether an external host receives your name, email address or accessibility information and why. Any optional disclosure for a host to send resources or future updates requires a separate

choice. We do not provide case files to event hosts. Event participants may see your display name and anything you choose to share; avoid discussing identifiable case details publicly.

We do not sell personal information. Identifiable information is not provided to funders or used in public reports merely because it would be useful. Any such disclosure requires a documented lawful basis, necessary safeguards and suitable privacy information.

7 Storage security and international transfers

We require role-based access, strong passwords, multi-factor authentication where available, secure transfer methods, device updates and suitable protection for stored records. Paper records must be secured. Team members must check recipients and attachments before sending, keep separate case records and report mistakes immediately.

Personal accounts, unauthorised cloud storage and unapproved software must not be used for client records. Identifiable case information must not be entered into AI tools, a documented lawful basis, suitable contractual safeguards and appropriate privacy information. Access is removed when a team member leaves or no longer needs it.

8 How long we keep information

We keep information only for as long as necessary for the documented purpose. The approved schedule must specify the periods and starting points below; these are not universal statutory retention periods.

Enquiries that do not become casework: 6 months
Active case records: for the duration of support; closed case records: 12 months.
Event registrations and accessibility information: 6 months after the event.
Complaints, safeguarding and breach records: Up to 5 years .

Newsletter details are kept while the subscription remains active, subject to periodic review. After an opt-out we retain only the minimal suppression record necessary to avoid contacting you again. Consent and authority records are kept for 12 months to demonstrate the relevant processing was authorised.

Longer retention requires a specific recorded reason, such as an ongoing safeguarding matter, complaint, legal claim or legal obligation, with a review date and restricted access. At the end of retention, information is securely deleted or genuinely anonymised.

9 Your rights

You can ask to access your information, correct inaccuracies, erase information, restrict its use or object to processing based on legitimate interests. Data portability applies where its legal conditions are met, including relevant automated processing based on consent or contract. These rights depend on the circumstances and are not all absolute. You can withdraw consent for consent-based processing and object to direct marketing at any time.

Contact the Data Protection Lead using the details in section 1. We normally respond to rights requests within one month, subject to lawful clarification, identity checks and any permitted extension. If an extension is necessary, we explain it within the required timeframe. We do not routinely charge a fee.

We check identity and authority proportionately. A parent does not automatically have a right to all of a child's records. We consider the child's rights, understanding and any necessary protection of other people's information. If we refuse part of a request, we explain the legal reason and how to challenge the decision.

Decisions about allocating support are made by people. We do not make decisions with legal or similarly significant effects solely through automated processing [confirm this reflects all systems used].

10 Complaints and data breaches

Please send privacy concerns or complaints to marnieh@send-empowerment.co.uk, addressed to the Data Protection Lead. You do not need to use a particular form. We acknowledge a data protection complaint within 30 days, make appropriate enquiries, keep you informed and respond without undue delay.

You may also complain to the Information Commissioner's Office at <https://ico.org.uk/make-a-complaint/> or by calling 0303 123 1113. You do not lose that right by using our complaints process.

All team members must immediately report suspected loss, unauthorised access, accidental disclosure or other personal data breaches to the Data Protection Lead. We contain the incident, assess the risk, document the facts and decisions and take corrective action.

Where required, we notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of a breach. Where a breach is likely to result in a high risk to people's rights and freedoms, we inform affected people without undue delay, unless a lawful exception applies.

11 Website cookies newsletters and online events

Our website privacy and cookie information must identify the actual hosting, form, analytics, translation and embedded-content providers, what they collect, their purposes, applicable bases and retention. Details and cookie notice link: [insert verified information]. Where consent is required under PECR, optional cookies or tracking are not activated until it is given. Users can change their choices.

Joining a newsletter or receiving general parent group invitations is optional and separate from asking for advocacy. Each promotional email provides an easy way to unsubscribe. We distinguish messages about a requested service or booking from promotional messages.

We explain any recording before an online session and identify the lawful basis, who will receive it and how long it will be kept. Participation does not by itself authorise publication of a person's image, voice or personal story. Recording practice and retention: [confirm, or state that sessions are not recorded].

12 Team responsibilities and review

Our Data Protection Leads oversees implementation, records of processing, legitimate interests assessments, provider checks, consent records, rights requests and incident handling. Everyone handling records must complete appropriate training before access and follow confidentiality, sharing and secure disposal requirements.

We assess whether a data protection impact assessment is required before introducing high-risk processing, new systems or significant changes, particularly where children's health information is involved. We document

applicable Article 9 and Schedule 1 conditions and maintain an appropriate policy document where required. We check whether ICO registration and a fee are required and keep any required registration current.

This service-user notice does not replace the separate privacy information required for volunteer recruitment, personnel records or other distinct activities. We review this policy annually and sooner when services, systems or law change. Updated versions are published on our website; material new uses are explained before they begin, with fresh consent where required.

Approval details to complete

Before publication, complete all bracketed fields and approve the proposed lawful bases against actual practice. Confirm the legal controller and address; provider names, locations and international transfers; retention and backup expiry; cookie and recording practices; and the named lead. Complete legitimate interests assessments and any required DPIA or appropriate policy document. Configure the form to retain consent evidence and update the old consent form so the documents agree.

Official guidance

ICO privacy notice generator <https://ico.org.uk/create-your-own-privacy-notice>

ICO special category data guidance <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/special-category-data/>

ICO Data Use and Access Act guidance <https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/data-use-and-access-act-2025/>

ICO personal data breaches guidance <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/>