



SENSE INCLUSION

Policy & Procedures

2026-2027

Privacy, Data Protection & Information Sharing

Version Number	Written by:	Approval date	Review date
6	L and J Slaterpartridge	Updated 04.09.2026	04.09.2027

Sense Inclusion C.I.C. • Robin Hill Country Park • Isle of Wight • www.sense-inclusion.org



Introduction

Sense Inclusion C.I.C. is committed to handling personal information lawfully, fairly and securely in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. This policy explains why we collect personal data, how we use and share it, how we keep it secure and how long we retain it.

Sense Inclusion C.I.C. collects and processes different information depending on the services being provided. This may include information about children and young people, parents/carers, staff, associates, volunteers, commissioners and other professionals.

If you have any questions on this Privacy Policy or otherwise relating to how we process your personal data, please address these to the directors at info@sense-inclusion.org

We will only collect and use personal data where there is a lawful reason to do so. Where information is required to provide a safe service, meet a legal or safeguarding duty, or fulfil a commissioned service, we may be unable to provide the service without it.

This policy will be reviewed annually, or sooner where legislation, guidance, systems or organisational arrangements change significantly.

Sense Inclusion may act as a data controller, joint controller or data processor depending on the circumstances and commissioning arrangements. Our role and responsibilities will be reflected in relevant contracts, data-sharing arrangements and privacy information.

Whose personal data do we collect?

By personal data we mean identifiable information about you, such as your name, email address, geographical postcode, mobile and home telephone number and your IP address.

We may also collect special categories of personal data about you such as details about your race or ethnic origin or data concerning your health, special educational needs, behaviour information and safeguarding information.

We only collect information that is relevant and necessary for the service being provided, safeguarding, legal duties, employment or organisational administration.

Personal data you provide to us.

From time to time you may provide to us personal data. This may be because you wish to:

- Use our services as an associate, learner, or client
- Provide services to us
- Otherwise contact us including with queries, comments or complaints.

You may provide personal data to us directly, or to us through our social media platforms.

We shall process all such personal data in accordance with this Privacy Policy. Certain personal data is mandatory to be provided to us in order that we can fulfil your request and we shall make this clear to you at the point of collection of the personal data.

If you provide personal data about a client under the age of 18, you confirm that either:

- (a) You are their teacher; tutor or local authority representative and you are entitled to provide the personal data to us.
- (b) You are the student's parent or legal guardian.
- (c) If you provide personal data about any other person, you confirm that you have their consent to do so.

All personal data that you provide to us must be true, complete and accurate. When you contact us by email or post, we may keep a record of the correspondence.

We may receive personal data from parents/carers, schools, Local Authorities, health and social care professionals, therapists, awarding organisations and other agencies involved with the child or young person. Information should only be shared where there is a lawful and appropriate reason to do so.

Lawful use of personal data

We will only use your personal data where we have a lawful basis to do so.

The lawful bases we may rely on include:

- Consent, where appropriate
- Contract or steps connected with a contract/commissioned service
- Legal obligation
- Legitimate interests, where appropriate

We may use or share personal data where necessary to comply with legal obligations, protect a child or adult at risk, respond to safeguarding concerns, deliver commissioned services, protect vital interests or support the legitimate interests of Sense Inclusion where these are not overridden by an individual's rights. Special category data is only processed where an additional lawful condition applies.

We may also use your personal data for our legitimate interests including to improve our services and in connection with any contracts or funding.

Consent is not always required before sharing information for safeguarding purposes. If seeking consent would place a child at increased risk, prejudice the prevention or detection of serious harm, or is otherwise not appropriate, information may be shared without consent where there is a lawful basis to do so.

Information will be shared on a need-to-know basis and only where it is necessary, relevant and proportionate. Staff should record significant safeguarding information-sharing decisions where appropriate.

Information sharing

Who do we share your data with?

We may share relevant information with organisations and professionals who need it to provide, commission, regulate or support our services. This may include schools, Local Authorities, health and social care professionals, therapists, awarding organisations such as AQA, contractors providing

approved services, and statutory safeguarding agencies. Only information that is necessary and proportionate will be shared.

We shall provide our service providers, only with such of your personal data as they need to provide the service for us and if we stop using their services, we shall request that they delete your personal data or make it anonymous within their systems.

We may from time to time need to provide personal data about a client to their teacher or local authority if there is a genuine need to do so.

Data protection law does not prevent appropriate information sharing to safeguard a child or young person.

Where there is a safeguarding concern, staff must follow the Safeguarding Policy and share relevant information promptly with the DSL and, where required, statutory agencies.

Secure transfer of personal information

Personal or sensitive information must be shared using an appropriately secure method. Where information is sent electronically, Sense Inclusion will normally use Egress secure email or another approved secure system.

Where Egress is not available or appropriate, files containing sensitive or confidential information must be password protected and the password shared separately from the document or email. Staff must check the recipient carefully before sending, particularly where information includes safeguarding, health, SEND, therapeutic or other special category data.

Storage and security of personal data

We shall process your personal data 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.

Data is stored using approved Sense Inclusion systems, including secure Microsoft services and other approved case-management, awarding-body or professional systems where required. Access is limited to those who need the information for their role.

Where specialist or therapeutic services require use of an approved professional system, information will be stored and processed in accordance with the relevant privacy and data-processing arrangements.

Any paper records containing personal data will be stored securely and access will be restricted. Sensitive information must not be left unattended or accessible to unauthorised persons.

Records will be retained only for as long as necessary in line with legal, safeguarding, contractual, insurance and organisational retention requirements. Safeguarding records will be retained and shared or transferred appropriately where required to protect children and support continuity of safeguarding information.

Access to personal data is restricted to staff and approved persons who need it for their role. Appropriate password protection, access controls and secure systems will be used. Staff must report

any suspected loss, inappropriate disclosure or data breach immediately to a director or the person responsible for data protection so that the risk can be assessed and, where required, reported to the Information Commissioner's Office within the statutory timescale.

All staff, associates and volunteers must protect confidential information, use approved systems, only access information required for their role, keep records accurate and up to date, and follow Sense Inclusion policies on safeguarding, IT safer use and confidentiality.

Staff responsibilities

Individuals have rights under data protection law. These rights apply subject to legal exemptions and the circumstances of the processing. For children and young people, rights may be exercised by the child where they have sufficient understanding, or by a person acting lawfully on their behalf.

- Right of access: You have the right to obtain from us a copy of the personal data that we hold for you.
- Right to rectification: You can require us to correct errors in the personal data that we process for you if it is inaccurate, incomplete, or out of date.
- Right to portability: You can request that we transfer your personal data to another service provider.
- Right to restriction of processing: In certain circumstances, you have the right to require that we restrict the processing of your personal information.
- Right to be forgotten: You also have the right at any time to require that we delete the personal data that we hold for you, where it is no longer necessary for us to hold it. However, whilst we respect your right to be forgotten, we may still retain your personal data in accordance with applicable laws.
- Right to stop receiving marketing information: You can ask us to stop sending you information about our services, but please note we shall continue to contact you in relation to any matters relating to your account, if you have one.

If you have concerns about how your personal data has been handled, please contact Sense Inclusion in the first instance. You also have the right to raise a concern with the Information Commissioner's Office (ICO).

Retention of personal data

Personal data will be retained only for as long as there is a lawful, safeguarding, contractual or operational reason to keep it. Different types of records have different retention periods.

Standard periods are set out in Appendix 1 – Data Retention Schedule.

Information will be securely deleted, destroyed, transferred or anonymised when it is no longer required. Where Sense Inclusion is acting as a data processor for a school or Local Authority, the relevant commissioning or data-processing agreement will take priority where it specifies return, deletion or retention requirements.

Appendix 1: Data Retention Schedule 2026–27

Supporting the Privacy, Data Protection & Information Sharing Policy

Purpose

This schedule supports the Sense Inclusion Privacy, Data Protection & Information Sharing Policy. It sets standard retention periods for the main records held by Sense Inclusion C.I.C. and should be used alongside any specific legal, safeguarding, commissioning, AQA, insurer or professional-body requirement.

The periods below are proportionate working periods for Sense Inclusion as a non-school alternative provision and therapy service. At the end of a retention period, records should be reviewed and securely deleted, destroyed, transferred or anonymised unless there is a clear lawful reason to keep them longer.

How to use the schedule

- Use the longest applicable period where a record falls into more than one category.
- Safeguarding information should be stored separately and treated under the safeguarding retention period.
- Where Sense Inclusion acts as a data processor for a school or Local Authority, follow the commissioning/data-processing agreement and return or delete data when instructed, unless there is another lawful reason to retain it.
- A short destruction log should be kept showing what was destroyed, when and by whom. The log should not contain unnecessary sensitive detail.
- When records containing personal or sensitive information are transferred electronically, use Egress secure email or another approved secure system. If this is not available or appropriate, password protect the file and share the password separately.

Children, young people and service delivery

Record type	Suggested retention	Action / notes	Basis
Referral/enquiry not taken forward	12 months after the enquiry/referral is closed	Delete securely unless needed for a complaint, safeguarding matter or future agreed referral.	SI schedule
Core AP learner file: referral information, EHCP copies, assessments, support plans, risk assessments, progress reports and commissioner correspondence	6 years after the final session / end of commissioned provision	Review before destruction. Safeguarding or clinical material follows the longer period below.	SI schedule
Attendance and session registers	6 years from the last entry	Suggested benchmark consistent with education record-keeping practice.	DfE benchmark
Safeguarding / child protection records	Until the child's 25th birthday	If records relate to child sexual abuse, retain until the child's 75th birthday. Review before destruction and retain longer where required by an ongoing case, inquiry or legal advice.	DfE / KCSIE
Therapeutic / play therapy clinical records for clients under 18	Until the client's 26th birthday	Reflects current PTUK retention guidance. Follow the practitioner's professional-body/insurance requirements where longer.	PTUK
Therapeutic / clinical records for clients aged 18+	6 years after therapy/support ends	Review against the practitioner's professional-body and insurer requirements.	SI schedule

Medication, medical support and individual health records	6 years after the provision ends	If part of a safeguarding or clinical record, use the longer safeguarding/clinical period.	SI schedule
Accident, significant incident and restrictive intervention records involving a child	Until the child's 26th birthday where injury/clinical risk is relevant; otherwise 6 years after the incident	If part of the safeguarding file, follow safeguarding retention. Significant claims/investigations may require longer retention.	SI schedule
Photographs / video / audio used for learning or authorised service purposes	Delete when the purpose ends; normally no later than 12 months after provision ends	Delete sooner if consent is withdrawn where consent is the lawful basis. If retained as safeguarding/clinical evidence, use that record's retention period.	SI schedule

AQA and learning evidence

Record type	Suggested retention	Action / notes	Basis
AQA Unit Award Scheme learner evidence, summary sheets and internal checking records	Keep until certification is complete and any AQA checking/spot-check requirement has passed; operational default 3 years after final claim	If AQA issues a current instruction requiring a different period, follow AQA. Keep only what is needed to evidence the claim.	AQA / SI
AQA certificate/claim administration records	5 years after certificate issue	Supports queries and replacement-certificate information; minimise personal data retained.	AQA / SI

Staff, recruitment and workforce

Record type	Suggested retention	Action / notes	Basis
Unsuccessful recruitment records	6 months after recruitment decision	Then delete unless there is a documented reason to keep longer.	SI schedule
Successful recruitment records / personnel file	6 years after employment or engagement ends	Includes contracts, references, supervision/management records and relevant employment correspondence unless another category requires longer.	SI schedule
DBS certificate copies / detailed certificate information	Normally no longer than 6 months after the recruitment decision	Do not retain full certificate information longer than necessary. Keep the check date, level, outcome/reference details needed for safer recruitment evidence.	DBS
Safeguarding allegations concerning staff/associates	Until normal retirement age or 10 years from the allegation, whichever is later	Keep separately/confidentially and follow current safeguarding/LADO guidance.	DfE / KCSIE
Staff training, safeguarding training and CPD records	6 years after employment/engagement ends	Longer where required by a professional body or where linked to an ongoing matter.	SI schedule
Driver declarations and vehicle compliance checks	6 years after driving duties for Sense Inclusion end	Current documents should also be reviewed/renewed at the frequency required by the Transport Policy.	SI schedule

Business, governance and data protection

Record type	Suggested retention	Action / notes	Basis
Contracts, commissioning agreements, invoices, receipts, bank/accounting records	6 years from the end of the relevant financial year / last payment	Longer where required by HMRC, an audit, ongoing transaction or legal matter.	HMRC / limitation
Complaints records	6 years after complaint closure	If the complaint includes safeguarding, staff allegations or clinical issues, retain under the longer applicable period.	SI schedule
Subject access / information-rights request records	2 years after the request is closed	HR-related requests may be retained with the relevant personnel record where necessary.	SI schedule
Personal data breach records	6 years after the breach record is closed / last updated	Keep enough information to evidence assessment, decisions and any ICO notification.	ICO / SI
Policies, procedures and superseded versions	6 years after superseded	Keep final approved versions, not unnecessary drafts.	SI schedule
Health & safety risk assessments and organisational incident logs	6 years after superseded / closed	Records concerning individual children may require the longer child/safeguarding period above.	SI schedule
Routine operational emails not forming part of another record	2 years, then review/delete	Important emails should be saved to the relevant case, personnel, contract or safeguarding record and follow that retention period.	SI schedule

Review, disposal and exceptions

- The schedule will be reviewed at least annually alongside the Privacy, Data Protection & Information Sharing Policy.
- Secure disposal means confidential destruction for paper records and secure deletion for electronic records. Backups should expire through normal secure backup-retention processes.
- Where there is litigation, a safeguarding investigation, police involvement, a complaint, insurance claim, coroner/court process, regulatory enquiry or subject access request, relevant records must not be destroyed until the matter is concluded and any further retention period has been considered.
- These are standard organisational periods, not a substitute for a specific legal, commissioner, AQA, insurer or professional-body requirement. Where a different requirement applies, that requirement should be followed and recorded.