

Data Protection and Information Security Policy

Solace SEND Support Ltd

Last reviewed: October 2026

Purpose

Solace SEND Support Ltd recognises that the information handled as part of SEND consultancy can be highly sensitive. This policy sets out the practical measures Solace uses to protect personal information.

Personal information

Solace may process information relating to parents and carers, children and young people, schools, Local Authority staff, professionals, clients and business contacts. This may include special category information relating to health, disability and SEND.

Access

Access to client information is restricted to information required for legitimate business purposes. Solace does not provide client information to family members, friends or other individuals unless there is an appropriate lawful basis or the client has authorised this.

Devices

Business information is accessed through a password, PIN and biometric protected laptop. The device uses security and anti-malware software. The device should not be left unattended while logged into systems containing client information.

Cloud storage

Client documents are stored using Microsoft OneDrive. Documents should be stored in appropriate client folders and should not be saved unnecessarily to unsecured locations.

Email

Solace uses its Google Workspace business email account, hello@solacesendsupport.co.uk. Sensitive documents should not be sent unnecessarily to personal email addresses. Where possible, clients may provide documents using secure cloud links rather than attaching large numbers of sensitive documents to emails.

Online meetings

Solace uses Microsoft Teams and Google Meet. Meeting links should not be shared publicly and should be provided only to intended participants.

Telephone

Business calls are made using VoIPfone. Sensitive information should be discussed by telephone only where reasonable privacy can be maintained.

Case tracking

Solace maintains a case-tracking spreadsheet through Microsoft Excel and OneDrive. The tracker should contain only information necessary to manage cases and business administration. Detailed clinical, educational or personal information should not be unnecessarily recorded in the tracker.

Paper records

Where paper records are created, they should be stored securely and not left where they can be accessed by unauthorised people.

Sharing information

Information should only be shared where there is a lawful basis and where sharing is necessary and proportionate.

Data breaches

Any suspected loss, accidental disclosure, unauthorised access or other data breach must be recorded and dealt with promptly under the Solace Personal Data Breach Procedure.

Review

This policy will be reviewed at least annually and whenever there is a significant change to Solace's systems or working practices.