STEP IN SUPPORT SERVICES

Data Protection, Confidentiality & Privacy Policy

Supporting Reintegration Every Step of the Year

Policy owner	Step In Support Services Directors
Approved by	Directors
Version	1.0
Effective from	October 2026
Review due	October 2027 or earlier if guidance/legislation changes

1. Purpose and scope

Step In handles personal and sometimes special-category information about children, families and professionals. We will process information lawfully, fairly, transparently, securely and only to the extent necessary for our service and safeguarding responsibilities.

This policy applies to all Step In directors, employees, sessional practitioners, associates, volunteers and contractors. It applies to work delivered in schools, homes, community venues, online where agreed, and other off-site locations.

Step In supports young people aged 11-18 through bespoke reintegration programmes combining attendance and engagement work, therapeutic/wellbeing support, educational support, social and personal development, family liaison and multi-agency working.

2. Information we may process

- Identity and contact details.
- School, attendance, educational and SEND information.
- Relevant health, wellbeing, risk and safeguarding information.
- Referral information, individual goals, session/engagement records and progress reviews.
- Parent/carer and professional contact/liaison records.
- Complaints, incidents and safeguarding records.

3. Data protection principles

- Lawfulness, fairness and transparency.
- Purpose limitation and data minimisation.
- Accuracy.
- Storage limitation.
- Integrity and confidentiality.
- Accountability and privacy by design.

4. Lawful basis and special-category information

The lawful basis will depend on the commissioning and processing context and may include contract, legal obligation, legitimate interests, vital interests or public task where applicable. Where special-category data is processed, Step In will identify an appropriate Article 9 condition. Consent will not be used as a default where another lawful basis is more appropriate. A data-protection record of processing should document the basis used for each main processing activity.

5. Children and transparency

Privacy information will be concise, clear and accessible. Young people will be told, in age-appropriate language, what information Step In holds, why it is used, who it may be shared with, how long it is kept and how they can raise a concern or exercise applicable rights. Parents/carers and commissioners will also receive appropriate privacy information.

6. Confidentiality and information sharing

- Therapeutic information is treated sensitively and is not routinely shared in unnecessary detail.
- Commissioners receive proportionate information needed for safeguarding, attendance, engagement, progress and agreed outcomes.

- Information may be shared without consent where lawful and necessary to protect a child or another person from harm.
- Only those with a genuine need should access sensitive records.
- Information-sharing decisions should be documented where significant.

7. Security

- Use secure, access-controlled systems and strong authentication.
- Avoid storing case information on personal devices or unapproved cloud services.
- Use secure methods when transferring sensitive information to schools or agencies.
- Report suspected data breaches immediately to a director/data-protection lead for assessment and, where required, notification.

8. Remote Communication and Data Security

Step In Support Services may provide remote therapeutic, educational, attendance and reintegration support. Remote delivery and electronic communication may involve the processing of personal and, where applicable, special-category information and must therefore be managed securely and confidentially.

- Remote sessions and professional communications must be conducted using appropriately secure and Step In or commissioner-approved platforms and communication channels wherever reasonably practicable.
- Practitioners must take reasonable steps to protect confidentiality when delivering remote sessions, including working from an appropriate private environment and taking reasonable precautions to prevent conversations or information being accessed by unauthorised individuals.
- Devices used for Step In work must have appropriate security measures, including password or equivalent access protection, and must not be left accessible to unauthorised individuals.
- Case information should not normally be downloaded, stored or retained on personal devices or unapproved cloud-storage services.
- Practitioners should only access, discuss or display information that is necessary for the purpose of the remote intervention.
- Personal or special-category information shared electronically with schools, families or other professionals must be shared through appropriately secure methods and only with individuals who have a legitimate need to receive it.
- Remote sessions will not normally be recorded, photographed or captured by screenshot by Step In practitioners. Any exceptional recording must have a legitimate professional purpose, appropriate authorisation and a clear lawful basis, with safeguarding, confidentiality, storage and retention requirements considered in advance.
- Young people and families should be advised that remote sessions should not be recorded, photographed, screenshotted or shared without prior agreement.
- Records arising from remote interventions, including relevant session notes, attendance or engagement information, safeguarding concerns and agreed actions, will be managed in accordance with Step In's wider confidentiality, security, retention and information-sharing arrangements.
- Any suspected loss, unauthorised disclosure, accidental sharing or other data-security incident arising during remote work must be reported immediately to the appropriate Step In director/data-protection lead and managed in accordance with Step In's data-breach procedures.

9. Retention and disposal

Step In will maintain a written retention schedule that reflects legal, safeguarding, contractual and insurance requirements. Records will not be kept indefinitely without reason. Secure deletion/destruction will be used when retention periods expire.

10. Individual rights and complaints

Requests relating to access, correction, erasure, restriction, objection or other applicable rights will be handled in accordance with data-protection law. Data-protection concerns may be raised at info@stepinsupportservices.org and individuals may also have the right to complain to the Information Commissioner's Office.

11. Website privacy notice - minimum publication information

- Who Step In is and how to contact us.
- Categories of information collected.
- Purposes and lawful bases.
- Recipients/categories of recipients.
- Retention approach.
- Individual rights and how to exercise them.
- Right to complain to the ICO.
- Any international transfers, automated decision-making or cookies/analytics where applicable.