

# Data Protection



## Processing of Special Category Data, Subject Access Rights and Data Breach Management

February 2026

Stepping Stones is fully committed to meeting its legal obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). We ensure that all personal data is handled lawfully, securely, and transparently in accordance with applicable data protection legislation.

Stepping Stones adheres to the seven principles of data protection. Personal data shall be:

1. **Processed lawfully, fairly and in a transparent manner.**
2. **Collected for specified, explicit and legitimate purposes** and not further processed in a manner incompatible with those purposes.
3. **Adequate, relevant and limited to what is necessary** in relation to the purposes for which it is processed (data minimisation).
4. **Accurate and, where necessary, kept up to date**, with reasonable steps taken to ensure inaccurate data is rectified or erased without delay.
5. **Kept for no longer than is necessary** for the purposes for which it is processed (storage limitation).
6. **Processed in a manner that ensures appropriate security**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage (integrity and confidentiality).
7. **Accountable.** We take responsibility for complying with the data protection principles and are able to demonstrate our compliance.

This policy applies to all individuals who process or have access to Stepping Stones' data in any format. This includes employees, trustees, volunteers, contractors, and any other individuals authorised to access Stepping Stones' ICT systems or records.

The policy applies to all personal data processed by Stepping Stones, whether held in paper or electronic form.

### Responsibilities

The Trustees has overall responsibility for ensuring that Stepping Stones complies with all applicable data protection legislation, including the UK GDPR and the Data Protection Act 2018. Day-to-day responsibility for data protection compliance is delegated to the Centre Manager.

All employees, trustees, volunteers, and contractors are responsible for:

- Familiarising themselves with and complying with this Data Protection Policy and related procedures.

- Promoting a culture of openness and continuous learning in relation to data protection compliance. Stepping Stones encourages the reporting of errors or concerns without the fear of blame. However, deliberate or reckless disregard of this policy may result in disciplinary action and, where appropriate, criminal proceedings.
- Ensuring the secure handling and safekeeping of personal data at all times, minimising the risk of loss, unauthorised access, or misuse. All staff must treat the personal data of others with the same care as they would their own.
- Accessing and processing personal data only on secure, password-protected devices and ensuring systems are properly logged off when not in use.
- Storing, transporting, and transferring personal data using appropriate security measures, including encryption and secure password-protected devices.
- Not transferring personal data offsite or onto personal devices unless expressly authorised and subject to appropriate safeguards.
- Deleting or securely disposing of personal data in accordance with this policy and Stepping Stones retention schedule.
- Informing Stepping Stones promptly of any changes to their own personal data (e.g., change of address, name or contact details).

Employees must direct any data protection queries or concerns to the Centre Manager. This includes, but is not limited to:

- Questions about the operation of this policy, data protection law, lawful bases for processing, data retention, data sharing, or data security.
- Concerns that this policy or data protection legislation is not being followed.
- Uncertainty about whether there is a lawful basis for processing personal data in a particular situation.
- Situations requiring consent to be obtained or recorded, responding to individuals exercising their data protection rights, or transferring personal data outside the UK.
- The discovery of a personal data breach or near miss. Immediate reporting is required in accordance with this policy.
- Engagement in any new activity, project, or system that may impact the privacy rights of individuals (a Data Protection Impact Assessment may be required).
- Proposals to share personal data with a third party acting as a data processor (e.g., contractors or service providers), where a compliant written agreement will normally be required.

## **Special Category Data and Criminal Offence Data**

In addition to identifying a lawful basis under Article 6 UK GDPR, the processing of special category data requires the identification of an additional condition under Article 9 UK GDPR and, where applicable, Schedule 1 of the Data Protection Act 2018.

Special category data includes personal data revealing an individual:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs

- Trade union membership
- Genetic data
- Biometric data used for identification purposes
- Health data
- Sex life or sexual orientation

Stepping Stones will only process special category data where a lawful basis under Article 6 applies and one of the following conditions under Article 9 (and Schedule 1 DPA 2018 where required) is met:

- The individual has given explicit consent for one or more specified purposes.
- Processing is necessary for carrying out obligations and exercising specific rights in the field of employment, social security, or social protection law.
- Processing is necessary to protect the vital interests of the individual or another person where the individual is incapable of giving consent.
- Processing is carried out in the course of legitimate activities by a not-for-profit organisation, relating solely to its members or those in regular contact with it, and the data is not disclosed externally without consent.
- The data has been manifestly made public by the individual.
- Processing is necessary for the establishment, exercise, or defence of legal claims.
- Processing is necessary for reasons of substantial public interest, including (but not limited to):
  - Safeguarding children or individuals at risk
  - Equality of opportunity or treatment
- Processing is necessary for the provision or management of health or social care.
- Processing is necessary for reasons of public interest in the area of public health.

Where reliance is placed on conditions relating to employment, health, research, or substantial public interest, Stepping Stones will also comply with the relevant provisions of Schedule 1 of the Data Protection Act 2018 and maintain an appropriate policy document where required.

Determining the correct lawful basis can be complex, and more than one condition may apply. Employees must consult the Centre Manager where there is any uncertainty.

Criminal offence data includes information relating to criminal allegations, proceedings, and convictions. Stepping Stones processes criminal offence data under Article 6 UK GDPR and a relevant condition under Schedule 1 of the Data Protection Act 2018, such as where processing is:

- Necessary for performing or exercising obligations or rights imposed by law in connection with employment, social security, or social protection;
- Necessary to protect the physical, mental, or emotional wellbeing of an individual; or
- Necessary for statutory purposes.

Appropriate safeguards will be implemented to ensure that such data is handled securely and confidentially.

## **Training**

All employees and relevant personnel who process personal data, particularly special category or criminal offence data, will receive appropriate data protection training. Training will be proportionate to their role and responsibilities and delivered in accordance with Stepping Stones training plan.

## **Record of Processing Activities (ROPA), Data by Design and Data Protection Impact Assessments (DPIAs)**

The ROPA is managed centrally by the Business Manager and is maintained and reviewed annually by all managers. Employees should be aware of the ROPA and understand its need to be updated as and when required.

Stepping Stones has a legal obligation to integrate appropriate technical and organisational measures into all its processing activities and to consider this aspect before embarking on any new type of processing activity. It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by a data protection impact assessment. Prior to the commencement of any such activity, employees must seek advice from the Centre Manager.

Stepping Stones will carry out a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of individuals, in accordance with Article 35 UK GDPR.

A DPIA will:

- Describe the nature, scope, context, and purposes of the proposed processing.
- Assess the necessity and proportionality of the processing in relation to its purpose.
- Identify and evaluate potential risks to the rights and freedoms of individuals.
- Identify measures and safeguards to mitigate and manage those risks, including security controls and compliance measures.

DPIAs will be reviewed at least annually where relevant, and sooner if there is a significant change to the processing activity, associated risks, or applicable legal requirements.

## **Data Breach Management**

Stepping Stones is committed to maintaining a robust and systematic process for identifying, reporting, and managing personal data breaches. All staff must report any actual, suspected, or potential data breach immediately. If there is any uncertainty about whether an incident constitutes a breach, it must still be reported to the Centre Manager or Business Manager without delay.

Appropriate technical and organisational measures are in place to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or access.

Under the UK GDPR, a personal data breach is defined as:

- A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
- A breach may be accidental or deliberate and may result in harm to individuals, reputational damage, service disruption, legal non-compliance, or financial loss.

Personal data breaches can include (but are not limited to):

- Sending personal data to the wrong recipient (email or post)
- Failing to use BCC where appropriate
- Sharing information without proper authority
- Loss or theft of devices (laptop, USB stick, tablet, phone) containing personal data
- Loss or theft of paper records
- Unauthorised access to systems or records
- Weak passwords or sharing login details
- Malware, hacking, or cyber-attacks
- Filing cabinets left unlocked
- Secure areas (e.g. server room) left open
- Improper disposal of confidential waste
- Website defacement
- Fire, flood, or other unforeseen events affecting records

A near miss is an incident that could have resulted in a breach but did not, such as an email sent to the wrong address that is returned undelivered. Near misses must also be reported so that risks can be reduced.

All staff; trustees, volunteers, and contractors are responsible for reporting actual, suspected, or potential data breaches immediately. Assisting with investigations where required and taking urgent action to prevent further damage where safe and appropriate.

The Centre Manager is responsible for overseeing the management of the breach.

If the breach involves IT systems (e.g. suspected hacking, malware, or network compromise), appropriate technical support must be contacted immediately.

Any individual who becomes aware of a personal data breach or near miss must report it immediately to the Centre Manager or Business Manager. If the incident occurs outside normal working hours, it must be reported as soon as reasonably possible.

Reports should include:

- What happened
- When it happened
- What type of data is involved
- How many individuals may be affected
- Whether the data has been recovered
- Any immediate action taken

Delays in reporting can increase risk and may result in regulatory non-compliance.

Stepping Stones will follow a structured response process.

**Preparation** - Ensuring staff are trained to recognise and report breaches and that appropriate resources are available.

**Identification** - Confirming whether a breach has occurred and assessing the nature, scope, and sensitivity of the data involved.

**Containment and Eradication:** Taking immediate steps to stop or limit the breach, recover lost data where possible, secure systems, prevent further unauthorised access and inform law enforcement if appropriate

**Risk Assessment:** Assessing the risk to the rights and freedoms of individuals, including potential distress, harm, identity theft, discrimination, or financial loss.

**Notification:** Where appropriate the ICO will be notified within 72 hours of becoming aware of a reportable breach.

- Affected individuals will be informed without undue delay where there is a high risk to their rights and freedoms.

All decisions regarding notification will be documented, including reasons where a decision is made not to notify the ICO.

**Recovery:** Restoring systems and returning to normal operations securely.

**Learning from Experience:** After the incident, Stepping Stones will review whether existing policies and procedures are adequate, is additional training is required and where personal data is held and how it is stored. It will also look at Whether security controls are sufficient, is data sharing arrangements are appropriate and whether technical safeguards need strengthening.

Improvements will be implemented where necessary to reduce the risk of recurrence.

The investigation process will begin immediately and, wherever possible, within 24 hours of the breach being discovered or reported.

See Appendix 2 for a copy of the data breach reporting form along with assessment.

## Monitoring and Compliance

Compliance will be monitored and reviewed regularly. Failure to comply with this policy may result in disciplinary action. Deliberate or reckless misuse of personal data may also result in legal and criminal consequences. Stepping Stones promotes a culture of openness and learning. Staff are encouraged to report genuine mistakes promptly so that risks can be managed effectively. A blame culture is discouraged; however, intentional misconduct will be addressed appropriately.

## Destruction of Records

Stepping Stones manages the retention and destruction of records in accordance with its Document and Records Management Policy and the principles of the UK GDPR.

Personal data will not be kept for longer than is necessary for the purposes for which it was collected. Once retention periods have expired, records will be securely and permanently destroyed.

- **Paper records** will be destroyed using secure disposal methods (e.g. cross-cut shredding or approved confidential waste services).
- **Electronic records** will be securely deleted in line with recognised data destruction standards.

Where third-party providers are engaged to destroy records on behalf of Stepping Stones, we will ensure that:

- The provider has appropriate accreditation and security safeguards in place.

- A compliant data processing agreement is in place where required.
- Secure certification of destruction is provided where appropriate.

Where electronic records are deleted with the intention of placing them beyond use, Stepping Stones will follow the Information Commissioner's Office (ICO) guidance on secure deletion and data "put beyond use," even if technical recovery may still be possible.

## Data Sharing

Stepping Stones will only share personal data where there is a clear lawful basis under Article 6 UK GDPR (and Article 9 where special category data is involved), and where such sharing is consistent with the organisation's Privacy Notice(s).

Personal data will only be shared where it is necessary, proportionate, and relevant to the purpose for which it is being disclosed.

**Safeguarding and Safety:** Stepping Stones may share personal data where necessary to protect the safety or welfare of children, parents, carer, staff, trustees, volunteers, beneficiaries, or others, in accordance with safeguarding obligations and legal requirements.

**Suppliers and Contractors (Data Processors):** Stepping Stones may share personal data with trusted suppliers and contractors who provide services on its behalf (for example, IT support providers, payroll services, or cloud storage providers). When doing so, Stepping Stones will:

- Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with data protection legislation.
- Put in place a written data processing agreement (either within the main contract or as a separate agreement) where required under Article 28 UK GDPR.
- Ensure that only the minimum personal data necessary is shared for the supplier or contractor to deliver their services, including any information necessary to ensure their safety while working with Stepping Stones.

**Law Enforcement and Public Authorities:** Stepping Stones may share personal data with law enforcement agencies, regulators, and government bodies where there is a lawful basis to do so, including:

- For the prevention or detection of crime and/or fraud.
- For the apprehension or prosecution of offenders.
- For the assessment or collection of tax or duties (e.g. HMRC requirements).
- In connection with legal proceedings or to establish, exercise, or defend legal claims.
- For research or statistical purposes, where the data is sufficiently anonymised or where appropriate consent has been obtained.
- With emergency services or local authorities to respond to an emergency situation affecting children, parent, carers, trustees, employees, volunteers, or others connected to Stepping Stones.

All data sharing decisions will be proportionate, documented where appropriate, and subject to appropriate safeguards to protect individuals' rights and freedoms.

## Data Subject Access Request (DSAR)

This section sets out how Stepping Stones handles requests from individuals who wish to access their personal data under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

This applies to all personal data processed by Stepping Stones in its role as a Data Controller, regardless of where the data is stored (electronic systems, emails, cloud storage, paper files, etc.).

**The Right of Access:** Under UK GDPR, individuals have the right to access their personal data, receive a copy of their personal data and understand how and why their data is being processed

This is known as a Subject Access Request (SAR). Individuals are also entitled to receive information about the purposes of processing, the categories of personal data concerned and who the data has been shared with. They are also entitled to know how long the data will be retained, whether any automated decision-making is taking place and if their data is transferred outside the UK and what safeguards apply

**Receiving a Request:** Subject access requests can be made in writing, by email, in person or through social media or other communication channels.

The individual does not need to mention “UK GDPR” or “Subject Access Request.” Staff are responsible for recognising when a request relates to personal data access.

All requests must be reported immediately to the Centre Manager or Business Manager.

**Time Limits:** A response must be provided within **one calendar month** of receiving the request. The time limit may be extended by up to **two additional months** if the request is complex or numerous. Any extension must be justified and the requester informed within the first month.

**Verifying Identity:** Before releasing any personal data, Stepping Stones must verify the identity of the requester. Acceptable identification may include a passport, driving licence, birth certificate and a utility bill or official letter confirming address.

Identification documents will only be used for verification purposes and will not be retained longer than necessary.

**Requests Relating to Children:** For children under 13, proof of parental responsibility (e.g. birth certificate) is required. Children aged 13 and over should normally submit their own request unless there is evidence they lack capacity.

**Fees:** In most cases, Stepping Stones cannot charge a fee for responding to a subject access request. A reasonable fee may only be charged where the request is manifestly unfounded; or excessive; or for additional copies of information already provided.

Any decision to charge a fee must be justified and documented.

**Searching for Personal Data:** All relevant personal data held at the time of the request must be considered. This includes all electronic records, emails, cloud systems, manual paper files, archived material and data held by third-party processors

Staff must make reasonable and proportionate efforts to locate the data. Searches should use appropriate search terms, include consultation with relevant staff and include data processors where applicable.

An audit trail should be maintained to demonstrate that a thorough search has been conducted.

**Deciding What Information to Provide** - Before disclosing information Stepping Stones will confirm that the data relates to the requester, remove information that is not relevant to the

request and protect the personal data of third parties by redacting identifying details where possible.

If third-party data cannot be separated, consider whether consent can be obtained or whether disclosure is reasonable in the circumstances.

There is no obligation to provide information already supplied to the individual or information that is exempt under data protection legislation.

Advice should be sought from the Centre Manager.

**Exemptions:** must be applied on a case-by-case basis. They should not be used automatically or as a blanket refusal.

Common exemptions may include:

- Personal data relating to third parties
- Manifestly unfounded or excessive requests
- Crime and taxation matters
- Legal professional privilege
- Confidential references
- Management forecasting or planning
- Ongoing negotiations
- Functions designed to protect the public
- Certain unstructured manual records

Before applying an exemption, appropriate guidance should be reviewed, including Information Commissioner's Office (ICO) guidance.

All decisions to apply exemptions must be documented.

**Providing the Response:** The response must be clear and easy to understand and avoid technical or legal jargon. It must be provided in a secure format. Where possible, the information should be provided in the requester's preferred format (e.g. electronic copy).

When sending personal data Stepping Stones will use secure email where available, password-protect attachments where appropriate, consider secure courier services for paper records and take extra care with special category or sensitive data.

**Complaints and Appeals:** If a requester is dissatisfied with the response, they have the right to request an internal review. The review will be carried out by an impartial person who was not involved in the original decision. Once the internal review is complete, the requester will be informed of the outcome. If they remain dissatisfied, they will be advised of their right to complain to the Information Commissioner's Office (ICO).

Stepping Stones is committed to handling subject access requests transparently, fairly, and in accordance with data protection legislation, while protecting the rights and freedoms of all individuals.

## Monitoring

Stepping Stones is responsible for the day-to-day implementation and oversight of this policy. The Centre Manager will monitor compliance and ensure that appropriate procedures, training, and safeguards are in place.

This policy will be formally reviewed annually, or sooner if there is a significant data protection incident, there are changes to relevant legislation or regulatory guidance; or operational changes require an update to procedures.

Any revisions will be approved in line with Stepping Stones' governance arrangements.

## **Complaints and Contact Details**

Stepping Stones is committed to maintaining high standards of data protection and transparency. We welcome feedback and take complaints seriously.

If you have concerns about how your personal data has been handled, please refer to our Feedback and Complaints Policy in the first instance.

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK supervisory authority for data protection.

However, the ICO generally expects individuals to raise their concerns with the organisation directly before contacting them.

Information Commissioner's Office (ICO)

Website: [www.ico.org.uk](http://www.ico.org.uk)

Telephone: 0303 123 1113

Address:

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Stepping Stones will cooperate fully with the ICO in the event of any investigation or regulatory enquiry.

# Training Plan



To meet the expectations of the information commissioner’s Office, Stepping Stones has a comprehensive training programme that covers data protection nationally and role specific. It covers the minimum:

- Handling requests
- Data sharing
- Information Security
- Data breaches
- Records Management
- Assign training based on job roles.
- Provide regular training to all staff, regardless of tenure, role, or level.
- Ensure all new employees undergo training before handling data and within one month of starting
- Obtain approval from senior management for the training programme.
- Establish agreed-upon timelines for training.
- Increase awareness through emails, posters, handouts, and blogs.
- Evaluate training through end-of-training assessments and feedback to enhance the training process.
- Process for employees who may miss training and follow-up.

## Role focussed Training

Regularity	Who it covers	What is covered	Material	Evidence of training
Annually	All employees	Identifying personal data and special category data. Importance of correct data management, Data breach process and reporting	Booklet	Signed completion stored in personnel files
As and when legislation changes or refresher if process not followed lawfully	Managers	Date by design and default / ROPA's / Culture of good practice	PowerPoint, discussion	Signed completion stored in personnel files

Annually	Admin	Recognising individual rights	Booklet with examples and questions	Signed completion stored in personnel files
Within one month of starting Stepping Stones	New employees	Identifying personal data and special category data. Brief overview of legislation. Data administration within Stepping Stones. Data breach process	Booklet and questions	Signed completion stored in personnel files
Sporadic	All employees and trustees	The use of attack simulation training. If fails, required to complete an online training video with questions.	Online	Report after training is completed stored on personnel file

Stepping Stones will raise awareness of the importance of data protection by providing updates and information to employees. This includes emails and posters around the office.

### **External training**

Any external training, where budget allows or is free will be investigated and brought in for all appropriate employees.

# Data Breach Reporting



## Appendix 2

### Confidential – GDPR Breach Record

Your Details	
Name	
Job title/role	
Email	
Details of Breach Discovery	
Date the breach was discovered	Click or tap to enter a date.
Time breach was discovered	
Date and time breach occurred	
Breach Description	
Type of breach (unauthorised access, loss/theft of device, accidental disclosure, hacking)	
Detailed description of incident	
How the breach was detected	
Personal Data Involved	
Categories of data (name, email, phone number, images)	
Number of data subjects affected	
Was there any personal data disclosed (health)	

Please ensure this record is now given to the Centre Manager or, Business Manager who will assess the risk and ensure appropriate steps are followed.

### Risk Assessment

Risk Factor	Description	Likelihood	Impact	Score	Notes
<i>Unauthorised access</i>	<i>Email received by wrong recipient</i>	<i>Possible</i>	<i>Minor</i>	6	<i>Risk is low. Only 1 email address. Other professional.</i>
		Choose an item.	Choose an item.		
		Choose an item.	Choose an item.		
Containment and Remediation					
Immediate steps taken to contain the breach					
Further actions planned/required					

Departments/individuals involved in containment	
<b>Notifications</b>	
Does the breach need to be reported to the ICO	Yes <input type="checkbox"/> No <input type="checkbox"/> Explain your reasons why it was, or wasn't reported to the ICO:
Date reported to the ICO	Click or tap to enter a date.
Has affected data subjects been notified	Yes <input type="checkbox"/> No <input type="checkbox"/>
Date data subjects were notified	Click or tap to enter a date.
How the data subjects were notified	
<b>Supporting Documents</b>	
Ensure all evidence is attached to form e.g., logs, screenshots and emails	
<b>Follow up Actions</b>	
Lessons learnt	
Responsible person to follow up	
Expected completion date	Click or tap to enter a date.
Name	
Signed	
Date	Click or tap to enter a date.