



IT POLICY

2026 – 2027

Document Title	IT Policy
Prepared By	Valmiro Fernandes
Approved By	Inderjot Singh
Effective Date	1st August 2026
Next Review Date	31st July 2027
Version	1

1. Purpose and Scope

Small Steps shall protect its information, maintain reliable systems and use technology responsibly. This policy applies to all authorised users of Company devices, networks, accounts and information, including approved remote access and personal devices. Child, clinical, safeguarding, employee and financial records require restricted access.

2. Access and Device Security

- Use an individual account and only the access necessary for your role. Sharing passwords, using another person's login and accessing records without a work purpose are prohibited. IT shall separate administrator accounts from routine user accounts.
- Use unique passwords or passphrases of at least 14 characters wherever supported and multifactor authentication for email, remote access and sensitive systems wherever available. Never disclose authentication codes or approve an unexpected login request.
- Lock screens whenever unattended. IT shall enforce automatic locking after no more than five minutes, encryption for portable devices, supported software, security updates and malware protection. Report any control that fails.
- Do not install unauthorised software, bypass security controls, connect unapproved storage devices or change network settings. Keep Company equipment secure and report loss, damage or theft immediately.

3. Information and Acceptable Use

Use approved systems for work records and approved business channels for sharing. Confirm the recipient and their authority, limit information to what is needed and use protected links or secure transfer for sensitive files. Do not send Company information to personal email, personal cloud storage or unapproved messaging groups.

Do not enter identifiable child, family, employee, clinical or confidential business information into public AI tools. Any AI use involving Company data requires prior approval, a documented privacy and security assessment and suitable provider safeguards. Staff remain responsible for checking outputs; AI shall not make unsupervised clinical or safeguarding decisions.

Unlawful content, harassment, fraud, unauthorised surveillance, personal commercial activity and deliberate security interference are prohibited. Personal phone use during child supervision is governed by the Digital Safeguarding and HR policies. Any permitted incidental use must not affect duties, safety, security or service quality.

4. Remote Access and Personal Devices

Remote access requires approval and the Company's secure connection method. Do not leave records visible or conversations audible to unauthorised persons. Personal devices may access Company data only with written approval and agreed security controls. Store data in the managed work environment and prevent personal backup or syncing. Any remote removal must be limited to Company data under the agreed arrangement; this policy does not permit unrestricted inspection or wiping of personal content.

IT Incidents Continuity and Accountability

5. Reporting and Responding to Incidents

Report suspected phishing, unauthorised access, malware, misdirected emails, missing equipment and data exposure immediately to IT and Operations through a known contact. If normal email is compromised, use telephone or another approved route. Report any child related concern to the DSL as well. Do not wait for proof or attempt to conceal an error.

If compromise is suspected, stop using the affected system and disconnect network access where safe. Do not wipe, reset, delete evidence or attempt unauthorised repairs. IT shall direct containment and preserve relevant logs. Suspected payment or bank detail changes must be independently verified using an established contact before any transfer.

Operations shall record the incident, appoint a response lead, involve the DSL, HR or data protection lead as relevant, assess harm and restore services safely. The data protection lead shall determine whether notifications to authorities and affected people are legally required and make them within the applicable timeframe. An internal report is not a substitute for statutory notification.

6. IT Management Controls

- Keep an inventory of devices, systems, approved software, suppliers and account owners. Approve access before joining, revise it when roles change and disable it promptly when access is no longer authorised, including at the agreed leaving time.
- Review access to sensitive systems at least quarterly. Apply critical security fixes promptly according to risk, and remove unsupported systems from service unless a documented, time limited exception and safeguards are approved.
- Back up essential records at least daily where the system allows. For supplier hosted systems, confirm backup and recovery arrangements. Keep a protected recovery copy separate from routine access and test restoration at least quarterly.
- Assess new suppliers and applications before use, including permissions, security, storage location, subcontractors, retention, deletion and any cross-border transfer requirements. Confirm appropriate contractual safeguards and lawful handling of health data.

7. Continuity Retention and Monitoring

Operations shall maintain a short outage plan with authorised alternative contact methods and secure temporary recording arrangements. Essential safeguarding and service information must remain available to authorised staff. Transfer temporary records into the approved system after recovery and dispose of copies securely.

Retain information according to the Company's approved retention schedule and any legal or safeguarding hold. Do not delete records to hide an incident. Monitoring of Company systems must be proportionate, lawful and explained to users. Access to personal information must be restricted to an authorised purpose.

Staff shall receive IT security induction and annual refresher guidance. Breaches may lead to access restriction for protection, a fair investigation and lawful disciplinary action. Management shall review incidents, recovery tests and exceptions annually.

Applicable Framework and Official References

Apply Federal Decree Law No. 45 of 2021 on Personal Data Protection where within scope, Federal Decree Law No. 34 of 2021 on Combatting Rumours and Cybercrimes, and any separate health data or licensing requirements. Read with the Data Protection, Digital Safeguarding and HR policies.

UAE Government data protection guidance

<https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws>

Privacy, Confidentiality, and Intellectual Property Rights (IPR) Statement

This document and all associated materials are the exclusive property of Small Steps Learning Difficulties Centre LLC (“Small Steps”) and are protected under the applicable laws of the United Arab Emirates, including but not limited to copyright, intellectual property, data protection, and contractual confidentiality obligations.

The contents of this document—whether in whole or in part—may include proprietary frameworks, clinical methodologies, internal policies, operational protocols, assessment tools, training content, or client-related information. All such content is considered confidential and is intended solely for authorised use by employees, contractors, partners, or stakeholders of Small Steps in connection with their official duties or approved collaborations.

Strictly prohibited actions include, but are not limited to:

- Copying, reproducing, or modifying the material without prior written authorisation;
- Distributing, sharing, or disclosing the content to unauthorised third parties;
- Using the document or its contents for commercial purposes or in a manner that could prejudice the interests of Small Steps or its clients; Removing this statement or any identifying information from the document.

All recipients are required to respect the confidentiality of information contained herein and to handle any personal or sensitive data in accordance with UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (PDPL), as well as Small Steps' internal policies on data protection and safeguarding. By accessing or utilising this document, you expressly acknowledge and agree to uphold these obligations and recognise the intellectual and proprietary rights of Small Steps Learning Difficulties Centre LLC.

If you have received this document in error, or if you are unsure of your authorisation to view or use its contents, you must immediately notify our Data Protection Officer by calling +971 52 854 6200 or emailing info@smallstepsbd.com