SCI POLICY: DATA PROTECTION POLICY

Functional Area:	Information Security & Data Protection
Owner (Name and Position):	Deborah McManamon, Data Protection Officer
Approved by:	Gareth Packham, Director of Information Security & Data Protection
Date of Approval:	October 2021
Version:	V4.0
Date for Review:	October 2022
Languages(inc. hyperlinks):	English
Applicable to:	Save the Children International ("SCI") employees, workers, volunteers, interns, consultants and member employees on secondment to SCI.

SECTION 1: PURPOSE

Save the Children International (SCI) is committed to using Personal Data responsibly and to ensuring that all Staff understand and comply with their responsibilities under this Data Protection Policy and the law, including the UK data protection legislation and any applicable local data protection legislation. SCA takes the GDPR as our standard, but where the principles of local data protection laws are more stringent than the principles contained in this policy, the principles of local data protection law should be applied.

SCI recognises that the correct and lawful treatment of Personal Data is a critical responsibility. Failure to adequately protect Personal Data could result in harm to others. It could also cause reputational damage to the Save the Children movement, loss of income or substantial financial penalties.

This Policy sets out the principles SCI applies in handling and safeguarding Personal Data entrusted to us and sets out the obligations of Staff in relation to the data that we gather and use. Staff members each have a responsibility in securing and protecting the Personal Data in SCI's care.

This Policy is mandatory for all Staff, and all Staff must read and comply with this Policy and any related procedures and guidance.

For any questions about this Policy, please contact SCI's Data Protection Officer (DPO) at dpo@savethechildren.org.

SECTION 2: POLICY STATEMENTS

1.	**Leadership & Oversight** A fundamental building block of accountability is strong leadership and oversight. This includes making sure that staff have clear responsibilities for data protection-related activities at a strategic and operational level. All employees and volunteers are responsible for following this policy when handling personal data. SCI's Senior Leadership Team (SLT) and Trustee Board have strategic accountability for data protection. The Audit & Risk Committee of the Trustee Board receives quarterly reports on data protection issues and risks. The Data Protection Steering Committee which is Chaired by the Chief Operating Officer and facilitated by the Chief Risk Officer, reports to SLT. SCI is required to have a Data Protection Officer, due to the nature of the personal data that we gather and use. The role of the DPO is to provide advice on and monitor compliance with this policy and SCI's legal obligations, advise on Data Protect Impact Assessments, and act as a contact point for data subjects and the Information Commissioner's Office in the UK. The DPO is the secretary of the Data Protection Steering Committee. The Data Protection team is assisted by a network of Data Protection Focal Points in Country Offices who support implementation at a local level. SCI is registered with the UK Information Commissioner's Office Registration No Z3214775.
2.	**Data Protection Principles** All use of personal data must follow the data protection principles, and we must be able to evidence that we are doing so. The principles are: a) **Lawfulness, Fairness and Transparency:** Personal Data must be processed lawfully, fairly and in a transparent manner. b) **Purpose Limitation:** Personal Data must only be collected for specified, explicit and legitimate purposes. c) **Data Minimisation:** Personal Data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. Where possible, SCI must apply anonymisation or pseudonymisation to Personal Data to reduce the risks to the Data Subjects concerned. d) **Accuracy:** Personal Data must be accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed e) **Storage Limitation:** Personal Data must be kept for no longer than is necessary for the purposes for which the Personal Data are processed. f) **Integrity and Confidentiality:** Appropriate technical or organisational measures must be in place to ensure the security of personal data, including protection against accidental or unlawful destruction, loss, alteration, unauthorised access, or disclosure.

	g) **Accountability:** Data Controllers must be responsible for and be able to demonstrate compliance with the principles outlined above. This includes being accountable for the personal data processed on our behalf. All Staff must follow these principles when gathering and using Personal Data.
3.	**Lawfulness of Processing** Whenever Personal Data is Processed, it must be done under one of the following **lawful bases**: a) the Data Subject has given their **consent** b) the Processing is **necessary for the performance of a contract** with the Data Subject c) the Processing is **necessary** to meet **legal obligations** d) the Processing is **necessary** to protect the Data Subject's **vital interests**; e) the Processing is **necessary** for the performance of a task carried out in the public interest; or f) the Processing is **necessary** to pursue SCI's **legitimate interests**. SCI must identify the lawful basis being relied on for each Processing activity and document this in our records **Consent** Consent will not always be the most appropriate lawful basis, but when it is relied upon, we must ensure that it is freely given, informed, specific and unambiguous. It should be clearly indicated by a statement or positive action. **Staff who are creating consent statements must follow the Consent Guidance.** **Children** SCI recognises that children require specific protection with respect to their Personal Data and we must ensure that the principle of fairness and the best interests of the child are central to all Processing of children's Personal Data. Consent is one possible legal basis for Processing children's Personal Data, but SCI recognises that sometimes using an alternative basis is more appropriate. Where Personal Data relates to a **child under the age of 18**, we must ensure that the child can understand the implications of the collection and processing of their Personal Data. If the child is not able to understand, an alternative basis should be used, or parental or guardian consent should be sought (unless this is not in the child's best interests).
4.	**Transparency** Transparency is fundamentally linked to fairness, and to the right that data subjects have to be informed about who we are, how and why we are using their personal data, and who else it is shared with.

	SCI is committed to being clear, open and honest with people from the start. This supports individuals to make informed decisions about the use of their data where this is appropriate, and to exercise their rights. When personal data is collected from children, we must provide them with information tailored for their age group so that they are able to understand what will happen to their Personal Data, and what rights they have. Staff who are involved in gathering or using personal data should familiarise themselves with privacy information and how to signpost people to it. Staff who are responsible for writing privacy information or making sure that it is provided must follow the Guidance on Transparency, or contact the Data Protection Officer for advice.
5.	**Training & Awareness** All Staff must undertake the mandatory data protection and information security training within 3 months of joining SCI. This must be refreshed every 12 months, or more frequently if directed. Staff in specialist roles may be required to take additional training to meet their responsibilities. There is addition information and guidance on OneNet here, and the Data Protection team is available to provide advice and guidance.
6.	**Individual Data Rights** Data Subjects (including children) have rights over their data, including the right to request a copy of their data from SCI, which is known as a 'subject access request' or SAR. If you receive a Subject Access or other request, please contact the data protection team by email tosubjectaccessrequest@savethechildren.org. You can also direct people to the form on our website. In the meantime, you **must not** disclose any information to the individual. The data rights under UK data protection legislation are: • **Right to be informed** Data Subjects have a right to know about SCI's Personal Data protection and data Processing activities, details of which will be contained in SCI's privacy notices. • **Right of access** Data Subjects can make what is known as a Subject Access Request ("SAR") to request a copy of their personal data. • **Right to rectification:** Data Subjects have a right to request that any incomplete or inaccurate information is corrected. • **Right to erasure (sometimes called the 'right to be forgotten')** Data Subjects have a right to request that SCI deletes data held about them, • **Right to restrict processing** Data Subjects can request that SCI stops processing their data for a particular purpose.

	• **Right to data portability** Data Subjects can ask SCI to provide copies of Personal Data held about them in a commonly used and easily readable format to transfer to another organisation (in limited circumstances: please consult the Data Protection Team for further details). • **Right to object** Data Subjects have the right to object to the use of their data in some circumstances. If their data is used for marketing purposes and they object, then the right is absolute and we must stop using their personal data to sell or promote things to them, or for fundraising. • **Rights in relation to automated processing:** Data Subjects have the right to challenge decisions and to request a review. • **Right to withdraw Consent** If SCI is relying on Consent to process their personal data, the Data Subject has the right to withdraw their Consent at any time.
7.	**Contracts & Data Sharing** When SCI uses third-party suppliers or service providers to process Personal Data on our behalf, we make sure that they have the appropriate measures in place to protect our data. This includes: • Conducting an assessment of their data protection and information security arrangements where appropriate • Ensuring that contracts include data protection clauses. Managers who are responsible for procurement decisions and contracting must make sure that they follow the agreed procedures and use the appropriate contract templates. **Data Sharing** For regular or routine sharing of personal data with other organisations that are not covered by a contract, we must agree the purpose for the sharing and the respective responsibilities are in relation to the data – for example responding to subject access requests. These should be set out in a Data Sharing Agreement. For requests for personal data from other organisations (including authorities or regulators) that are not covered by a contract or Data Sharing Agreement please seek the advice of the Data Protection Team.
8.	**Risk & Data Protection Impact Assessment** Data Protection Impact Assessment is a process to help identify and minimise data protection risks, particularly when implementing new processes or systems. It **must** be done by when there is a high risk to individuals and for some specific types of processing – including location tracking, providing online services to children, and processing biometric or genetic data. More detailed information on this is provided in the Guidance on DPIAs. Process and system owners are accountable for following this Guidance.

	Where a DPIA addressing the data protection and information security risks has already been conducted for a similar project or programme and is deemed applicable to the intended processing, a further DPIA may not be required – but managers must seek the advice of the Data Protection Team so that this can be documented.
9.	**Records Management & Security** Good records management supports good data governance and data protection. Information security also supports good data governance, and is itself a legal data protection requirement. Poor information security leaves our systems and services at risk and may cause real harm and distress to individuals. All staff must comply SCI's Acceptable Use of IT Policy which sets out in more detail the relevant precautions Staff are required to take to ensure data security, including the secure use of email, internet and mobile devices. We have a Data Classification Policy to help us ensure that we appropriately control access to our data and all staff and volunteers who produce documents and records should follow this policy. We maintain a record of our uses of personal data across the organisation and this is managed by the Data Protection team.
10.	**Data Retention** As a principle, personal data should only be kept for as long as necessary for the purposes for which it was collected. This retention period should be set when the data is first gathered or used, and should be explained to the data subjects in the privacy notice. The following must be taken into account when setting retention periods: • Whether there are any legal obligations to retain the data or records for a specific minimum period. • Whether we have any contractual obligations which set out how long we should keep records and how they should be dealt with at the end of the period. • Whether there is a specific business need that needs to be met. When reviewing data and records for disposal, decision makers should also consider whether the data or records may have enduring value to the organisation, or wider society which could justify their continued retention. Data retention periods must be included in contracts or agreements with suppliers or partner organisations who are acting on our behalf, and contract managers must ensure that SCI's instructions are followed and that data is returned to us or deleted at the end of the contract unless otherwise agreed. For more detailed guidance please refer to the Records Retention Policy and Schedule which sets out minimum retention periods for specific types of records.

11.	**International Data Transfers** SCI must ensure that adequate safeguards are in place before personal data is transferred internationally. This includes where SCI is acting as a data processor on behalf of SC Members. New processes which potentially include transfers of Personal Data should not be initiated without prior consultation with the Data Protection Team.
12.	**Breach Response & Monitoring** A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A breach may result from the loss or theft of the data itself, or the equipment or device on which it is stored, such as a laptop or phone. Data incidents are managed by the Information Security and Data Protection team. Actual or suspected data breaches must be reported using the Datix incident management system as soon as possible and ideally within 12 hours. This is so we can quickly take steps to reduce the risk to individuals, and to meet our obligations to notify the Regulator where this is appropriate.
13.	**Policy Breaches** If you suspect that this Policy may have been breached in any other way, please contact the DPO at dpo@savethechildren.org. Alternatively, you may wish to follow SCI's Whistleblowing Policy and Procedures. Breaches of this Policy may result in disciplinary action.

SECTION 3: DEFINITIONS

Please refer to the Data Protection Glossary

SECTION 4: RELATED DOCUMENTS

DOCUMENT	LOCATION
SCI_IT_DP_Data_Protection_Glossary	SCI Quality Framework
SCI_IT_DP_DPIA_Guidance_EN	SCI Quality Framework
SCI_IT_DP_Transparency_Guidance_EN	SCI Quality Framework
SCI_IT_DP_Consent_Guidance_EN	SCI Quality Framework
SCI_IT_DP_Records_Retention_Policy_EN	SCI Quality Framework
Child Safeguarding Policy	

Code of Conduct	
Whistleblowing Policy and Procedure	
Acceptable Use of IT Policy	
IT Security Policy	
SCI Privacy Notice	SCI Website
Subject Access Request Form	SCI Website