

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 2022
Version:	V5.0
Date for Review:	October 2023
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 there is local legislation that has differing or more stringent requirements than those set out in this policy, those local requirements must be complied with.

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.	<p>Leadership & Oversight</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The Data Protection team is assisted by a network of Data Protection Focal Points in Country Offices who support implementation at a local level.</p> <p>SCI is registered with the UK Information Commissioner's Office Registration No Z3214775.</p>
2.	<p>Data Protection Principles</p> <p>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:</p> <ul style="list-style-type: none"> 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

	<p>e) Storage Limitation: Personal Data must be kept for no longer than is necessary for the purposes for which the Personal Data are processed.</p> <p>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.</p> <p>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.</p> <p>All Staff must follow these principles when gathering and using Personal Data.</p>
3.	<p>Lawfulness of Processing</p> <p>Whenever Personal Data is Processed, it must be done under one of the following lawful bases:</p> <ul style="list-style-type: none"> 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. <p>SCI must identify the lawful basis being relied on for each Processing activity and document this in our records</p> <p>When the personal data includes 'special category' data (personal data which requires heightened data protection measures due to its sensitive and personal nature) we also need to have an additional justification (as set out in the legislation) for using that data.</p> <p>Consent</p> <p>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.</p> <p>Staff who are creating consent statements or managing processes which rely on consent must follow the Consent Procedure and refer to the Consent Guidance which provides supporting information.</p>

	<p>Children's Data</p> <p>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.</p> <p>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).</p>
4.	<p>Transparency</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Staff who are involved in gathering or using personal data should familiarise themselves with privacy information and how to signpost people to it.</p> <p>Staff who are responsible for writing privacy information or making sure that it is provided must ensure that it includes all the elements in UK GDPR or other applicable legislation by referring to the Transparency Guidance and following the Privacy Information Procedure in the Quality Framework.</p>
5.	<p>Training & Awareness</p> <p>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.</p> <p>Staff in specialist roles may be required to take additional training to meet their responsibilities.</p>

	<p>There is additional information and guidance on OneNet here, and the Data Protection team is available to provide advice and guidance.</p>
6.	<p>Individual Data Rights</p> <p>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.</p> <p>If you receive a Subject Access or other request, please contact the data protection team by email to subjectaccessrequest@savethechildren.org. You can also direct people to the Privacy Notice on our website where they can find more information. In the meantime, you must not disclose any information to the individual.</p> <p>The data rights under UK data protection legislation are:</p> <ul style="list-style-type: none"> • 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.	<p>Contracts & Data Sharing</p> <p>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:</p> <ul style="list-style-type: none"> • Conducting an assessment of their data protection and information security arrangements where appropriate • Ensuring that contracts include appropriate data protection clauses. <p>Managers who are responsible for procurement decisions and contracting must make sure that they follow the agreed procedures and use the appropriate contract templates.</p> <p>Data Sharing</p> <p>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.</p> <p>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.</p>
8.	<p>Risk & Data Protection Impact Assessment</p> <p>Data Protection Impact Assessment is a process to help identify and minimise data protection risks, particularly when implementing new processes or systems.</p> <p>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 DPIA Procedure and supporting guidance.</p> <p>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.</p>

9.	<p>Records Management & Security</p> <p>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.</p> <p>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.</p> <p>We maintain a record of our uses of personal data across the organisation and this is managed by the Data Protection team.</p>
10.	<p>Data Retention</p> <p>As a principle, personal data should only be kept for as long as necessary with reference to the purpose for which it was collected and to meet any specific record keeping obligations. 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.</p> <p>The following must be taken into account when setting retention periods:</p> <ul style="list-style-type: none"> • 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 to be met. <p>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.</p> <p>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.</p> <p>For more detailed guidance please refer to the Records Retention Procedure and Schedule which sets out minimum retention periods for specific types of records.</p>

11.	<p>International Data Transfers</p> <p>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.</p> <p>New processes which potentially include international transfers of Personal Data should not be initiated without prior consultation with the Data Protection Team.</p>
12.	<p>Breach Response & Monitoring</p> <p>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.</p> <p>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.</p> <p>Data incidents are managed by the Information Security and Data Protection team.</p> <p>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 UK regulators and/or regulators in other jurisdictions where applicable.</p>
13.	<p>Policy Breaches</p> <p>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.</p> <p>Breaches of this Policy may result in disciplinary action.</p>

SECTION 3: DEFINITIONS

Term	Definition
------	------------

Anonymisation	<p>As used in GDPR and UK GDPR</p> <p>The process of removing information or features from data which would allow it to be used to identify 'data subjects'. If the data is rendered in such a manner that the Data Subject is not, or no longer, identifiable then data protection legislation does not apply.</p> <p>When considering whether data has been anonymised, we must take into account all the means reasonably likely to be used, by ourselves or a third party, to identify an individual that the information relates to.</p> <p>The process of removing from data information or features which would allow it to be used to identify the Data Subject from which it was gained. The data is rendered in such a manner that the Data Subject is no longer identifiable.</p> <p>Note that we need to be aware of the possibility of re-identification, and of risk to groups and communities arising from data even where no individuals can be identified.</p>
Availability	<p>Data is accessible and usable by those who are authorised to access it whenever needed. Loss of availability of data, even if not disclosed or accessed by others, could constitute a data breach.</p>
Biometric data	<p>As defined in GDPR and UK GDPR</p> <p>Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic* data</p> <p>*fingerprint</p>
Confidential data	<p>Data which is not public knowledge, and which is shared or disclosed in circumstances which create an obligation for it to be kept confidential (for example subject to a non-disclosure agreement or due to the relationship between the parties involved).</p> <p>Note that marking data or documents as 'confidential' may be a useful indicator of how they should be treated, but it will not necessarily protect the information it from disclosure in all circumstances (for example if an individual makes a subject access request under GDPR or other data protection legislation).</p>

Consent	<p>As defined in GDPR and UK GDPR</p> <p>Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;</p>
Data concerning health	<p>As defined in GDPR and UK GDPR</p> <p>Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status</p>
Data Controller	<p>As defined in GDPR and UK GDPR</p> <p>The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data</p>
Data Processor	<p>As defined in GDPR and UK GDPR</p> <p>A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;</p>
Datix	<p>Datix is a cloud-based incident reporting and case management system. All incidents related to Fraud, Child Safeguarding, Adult Safeguarding, Safety & Security, Medical, IT Security and Data Protection in SCI should be reported in Datix.</p>
Data Protection Impact Assessment (DPIA)	<p>As used in GDPR and UK GDPR</p> <p>A process to identify and mitigate risks to individuals arising from the processing of personal data, taking into account the nature, scope, context and purposes of the processing and the sources of the risk.</p>
Data Protection Officer	<p>As used in GDPR and UK GDPR</p> <p>An Officer appointed to monitor compliance with data protection obligations, advise on Data Protection Impact Assessment and other processes, and act as a contact point for data subjects and supervising authorities. The organisation itself remains responsible for complying with data protection legislation.</p> <p>The SCI Data Protection Officer can be contacted at dpo@savethechildren.org</p> <p>Legislation in some other jurisdictions also requires the appointment of a Data Protection Officer or similar role.</p>



Filing system	<p>As defined in GDPR and UK GDPR</p> <p>Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis</p>
Genetic data	<p>As defined in GDPR and UK GDPR</p> <p>Personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.</p>
Information Asset	<p>A body of information that can be managed as a single unit, with recognisable content and value. An information asset can be in any format.</p>
Information Asset Owner	<p>The owner of an information asset with responsibility for ensuring that it is handled in accordance with SCI policies and supporting guidance and procedures.</p> <p>The IAO should be a senior responsible person in the relevant business directorate or function.</p>
Information security	<p>As defined by NIST (US Dept of Commerce)</p> <p>Protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide:</p> <ul style="list-style-type: none"> • Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity • Confidentiality, which means preserving authorised restrictions on access and disclosure, including means for protecting personal privacy and proprietary information • Availability, which means ensuring timely and reliable access to and use of information
Information society service	<p>As defined in Directive (EU) 2015/1535 of the European Parliament and of the Council</p> <p>Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.</p>
International organisation	<p>As defined in GDPR and UK GDPR</p> <p>An organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.</p>



Information Commissioner's Office (ICO) (UK)	<p>The Information Commissioner's Office (ICO) is the UK's independent public body which regulates information rights in the public interest.</p> <p>As well as data protection legislation (UK GDPR and the Data Protection Act 2018), it regulates legislation relating to PECR (electronic communications), eIDAS (electronic transactions), NIS (national infrastructure security), Re-use of Public Information, and Investigatory Powers. In England, Wales and Northern Ireland only the ICO also regulates Freedom of Information, Environmental Information, and INSPIRE legislation.</p>
Legal Professional Privilege (England & Wales)	<p>The protection from disclosure of certain confidential communications (including email):</p> <ul style="list-style-type: none"> • Between lawyers (including in-house) and clients for the sole or dominant purpose of giving or receiving of legal advice (Legal Advice Privilege) • Between lawyers (including in-house) or their clients and any third party for the sole or dominant purpose of obtaining advice or information in connection with existing or reasonably contemplated adversarial litigation (Litigation Privilege) <p>Some provisions of UK Data Protection legislation in the UK, including the Right of Access, do not apply to legally privileged information.</p>
Personal Data	<p>As defined in GDPR and UK GDPR</p> <p>Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>
Personal data breach	<p>As defined in GDPR and UK GDPR</p> <p>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.</p>
Processing	<p>As defined in GDPR and UK GDPR</p> <p>Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.</p>



Profiling	<p>As defined in GDPR and UK GDPR</p> <p>Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.</p>
Pseudonymisation	<p>As defined in GDPR and UK GDPR</p> <p>The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.</p>
Recipient	<p>As defined in GDPR and UK GDPR</p> <p>A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with [UK domestic law or Union or Member State law] shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.</p>
Restriction of processing	<p>As defined in GDPR and UK GDPR</p> <p>The marking of stored personal data with the aim of limiting their processing in the future.</p>
<p>Special Category Data</p> <p>(sometimes referred to as sensitive personal data)</p>	<p>As used in GDPR and UK GDPR</p> <p>A sub-category of personal data that requires heightened data protection measures due to its sensitive and personal nature.</p> <p>Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.</p> <p>Note that in other jurisdictions the special category or sensitive personal data may include other categories – for example in the Uganda Data Protection and Privacy Act 2019 financial data is included; and in the Kenya Data Protection Act 2019 it includes property details, marital status, family details including names of the person's children, parents, spouse or spouses.</p>



Third Party	<p>As defined in GDPR and UK GDPR</p> <p>A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.</p>
Records of Processing Activities	<p>As used in GDPR and UK GDPR</p> <p>Output of a data mapping exercise. Formal documentation kept by a Data Controller or Data Processor of uses of personal data across the organisation.</p> <p>Records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. This must be made available to authorities upon request.</p> <p>In some other jurisdictions there are similar requirements to keep and/or submit details of processing to supervisory authorities.</p>
Subject Access Request (SAR)	<p>As used in GDPR and UK GDPR</p> <p>A request from a 'data subject' for a copy of their personal data held by a Data Controller.</p>

SECTION 4: RELATED DOCUMENTS

DOCUMENT	LOCATION
SCI_IT_DP_DPIA_Guidance_EN	SCI Quality Framework
SCI_IT_DP_DPIA_Procedure_EN	SCI Quality Framework
SCI_IT_DP_Transparency_Guidance_EN	SCI Quality Framework
SCI_IT_DP_Privacy_Information_Procedure_EN	SCI Quality Framework
SCI_IT_DP_Consent_Guidance_EN	SCI Quality Framework
SCI_IT_DP_Consent_Procedure_EN	SCI Quality Framework
SCI_IT_DP_Records_Retention_Procedure_EN	SCI Quality Framework
Acceptable Use of IT Policy	SCI Quality Framework
IT Security Policy	SCI Quality Framework
SCI Privacy Notice	SCI Website