Data Protection Policy

1. Aims of this Policy

Safe Child Thailand (***SCT***) needs to keep certain information on its employees, trustees, volunteers, interns, beneficiaries, donors, businesses, religious organisations and other supporters to carry out its day to day operations, to meet its objectives and to comply with its legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998 (***DPA***) and the Privacy and Electronic Communications Regulation (***PECR***) in the United Kingdom and the Data Protection Act of 1988 and Data Protection Amendment Act of 2003 in Ireland as well as the requirements of the EU General Data Protection Regulation (***GDPR***). To comply with the relevant legislation, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers staff, trustees, associates, consultants, interns, volunteers and representatives (the ***SCT persons***).

In line with the data protection principles, SCT will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for specific, explicit and lawful purposes;
- Be used and disclosed only in ways compatible with these purposes;
- Be adequate, relevant but not excessive;
- Be accurate and kept up to date;
- Not be held longer than necessary;
- Be processed in accordance with the rights of data subjects;
- Be subject to appropriate security measures;
- Not be transferred outside the European Economic Area (***EEA***) unless specific criteria are met; and
- Be provided to individuals upon their request.

How these principles are implemented is set out in the follow paragraphs.

2. Processing Data in accordance with the principles

Processing is obtaining, recording, using, holding, amending, disclosing, destroying and deleting personal data. In essence, processing data means undertaking any kind of

operation on data. This includes some paper-based personal data as well as that kept electronically. The organisation will seek to abide by the relevant legislation and the DPA principles in relation to all the personal data it processes. In order to adhere to these principles, the following must be considered:

2.1. Be obtained fairly and lawfully and shall not be processed unless certain conditions are met

Any personal data obtained by SCT must be obtained in accordance with this Data Protection Policy, which outlines the following information:

- the name of the data controller;
- the purpose in collecting the data;
- the persons or categories of persons to whom the data may be disclosed;
- whether replies to questions asked are obligatory and the consequences of not providing replies to those questions;
- the existence of the right of access to their personal data;
- the right to rectify their data if inaccurate or processed unfairly; and
- any other information which is necessary so that processing may be fair and to ensure the data subject has all the information.

The Data Protection Policy will be provided upon request and is easily accessible on SCT's website. It is also linked to any online donation forms created by SCT.

If for any reason data is collected by a third party in the name of SCT, the Data Protection Policy must be provided to the individual upon collection of data if they request it. Clear records of consent to collect the information of and for SCT to contact individuals must be provided by the third party.

When processing sensitive data (i.e. birth status, disability status, marital status, religion, health status, etc.) consent must be obtained from the individual. If they are unable to do so (because of incapacity or age) consent must be given by a parent or guardian stating that the individual has been informed of the purpose/s for processing their data and they have consented to the data processing.

2.2. Be obtained for a specific, explicit and lawful purpose

SCT will fully disclose their purpose when collecting data from individuals. Explicit consent must be gained from the individual in the case of direct marketing.

Before personal information is collected, we will consider:

- Legal necessity of the information;
- Necessity of data for contact with each individual; and
- Necessity of data to complete service provision for the individual.

We will inform people whose information is gathered about the following:

- The fact that their information will be entered into our database and kept for a reasonable and appropriate time period. We will regularly review (on at least a yearly basis) what information we possess on our database to ensure that information is not kept for longer than necessary;

- That their information will be used for payment processing purposes; and
- That their information will be used for direct marketing purposes if they have opted-in.

Privacy notices will be provided to the individuals by the following means:

- The privacy notice will be displayed on the website along with the full Data Protection Policy and Safeguarding Policy;
- The privacy notice will be displayed on all electronic donation forms; and
- The privacy notice will be included in donor welcome and sponsor welcome packs.

Fields exist in the SCT database which indicate certain sets of data and the specific purpose for which that data can be used. When using data for a specific purpose, only data that was collected for the specific purpose will be used.

2.2.1. Consent

SCT requires individual consent before sending direct marketing materials. Consent must be:

- Freely given and the individual must have a genuine choice over whether or not to consent to marketing;
- Specific – consent must be specific to the type of direct marketing they are being contacted through (i.e. mail, email, text...);
- Informed, i.e. the person must understand what they are consenting to; and
- An unambiguous indication of the individual's wishes, i.e. consent must be a positive expression of choice.

2.2.2. Implied consent

SCT recognises that implied consent does not apply to direct marketing. Notifications in a Privacy Policy or other implicit means do not ensure consent. As such SCT will ensure that consent is obtained explicitly for all contacts.

2.2.3. Opt-in and opt-out

In gaining consent, SCT will provide unchecked opt-in boxes for each method of communication used for direct marketing. Consent must be secured for the specific method of communication before they will be contacted by that method for marketing purposes.

In the case of online forms, SCT will also provide a prominent statement stating: "By submitting this form, I consent for SCT to contact me in accordance with the terms of the charity's Privacy Policy".

2.2.4. Indirect (third party) consent

When using third-party mailing lists SCT will complete due diligence to ensure that consent was given in accordance with the DPA and PECR regulations.

2.2.5. Proof of consent

Under the DPA and GDPR, organisations can be at risk of enforcement action unless it can demonstrate that people they contact have given valid consent.

SCT will keep clear records of exactly what donors have consented to. This will include a database record of consent detailing the date of consent, the method of consent, who obtained consent, and exactly what information was provided to the person consenting.

Individuals have the right to withdraw consent at any time.

2.3. Be used and disclosed only in ways compatible with these purposes

SCT will only use and disclose information when it is compatible for the purpose for which it was collected (i.e. mailing information disclosed to third-party printers for direct mailing). SCT will also obtain the individuals consent to process their personal data in the form of a signature or online submission before data is processed. Data will also be suppressed upon termination of an individual's relationship with SCT (see section 2.6 on Suppression below).

2.3.1. Third party access to personal data

Personal data will never be shared with third parties unless necessary to fulfil requirements of SCT's work. Third party exceptions may include:

- Web designers;
- Donation processing companies;
- Mailing houses;
- Graphic designers;
- Public Relations consultants; and
- Relevant government offices.

2.4. Be adequate, relevant but not excessive

SCT may process the following personal data:

- Bank details of service-providers, consultants and partners;
- Bank, credit-card and financial details (i.e. tax-payer status) of donors;
- Personal data of donors (i.e. names, month of birth, marital status, PPS numbers for Irish donors etc.);
- Contact details of donors (i.e. addresses, email addresses and telephone numbers etc.);
- Personal data of beneficiaries (i.e. names, d.o.b, sex, birth status, disability status, marital status, religion, health status etc.);
- Contact details of beneficiaries (ONLY project location);
- Information relating to SCT persons; including, salary, bank details, contact information, personal and employment data, criminal record status etc.;
- Photographs of beneficiaries in Thailand and surrounding countries;
- Photographs of donors and fundraisers in the UK and around the world;
- Case histories and personal stories of vulnerable children and adults;
- Relevant documents, passwords, online accounts, files, computer data, photographs, technical data and other information, which are the property of SCT; and

- Account information for social media, online platforms and digital communications.

Personal sensitive information will not be used apart from the exact purpose for which permission was given. Sensitive information includes information relating to:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Health or sex life and sexual orientation;
- Genetic data; and
- Biometric data where processed to uniquely identify a person.

Personal data is kept in the following forms:

- Salesforce Database (password protected with limited employee access to data based on need);
- On the SCT server (encrypted);
- Compact discs holding beneficiary data;
- Computer files (password protected log-ins);
- Printed files; and
- Printed copies of case studies of beneficiaries.

Groups of people within SCT who will process personal data are SCT persons as well as third party consultants (i.e. web design, donation processors, mailing houses, designers, PR staff).

To ensure that these minimum requirements are relevant a yearly review will be conducted by SCT. This review will examine data solicited through various forms and online media and well as examining personal details already held on the SCT database and print files.

2.5. Be accurate and kept up to date

SCT will ensure that all personal data is accurate and kept up-to-date.

We will take the following measures to ensure that personal information kept is accurate:

- Vetting donor data through mailing services prior to all mailings (done by mailing house);
- Periodic data cleansing by a third party to ensure donor data is current. The third party contractor will not be allowed to use any of the data being processed beyond checking for accuracy. Data will be checked through the following means:
    - Active Line Testing;
    - Address Cleansing;
    - Email Validation;
    - TPS/CTPS screening;
    - MPS screening; and/or
    - FPS screening; and

- Suppression of incorrect information.

To do so, SCT will employ clerical and computer procedures to ensure there is appropriate cross-checking of data including utilising database fields correctly for communications and making updates to personal data in a timely manner.

Periodic data cleansing will take place to ensure that all data is up-to-date including mailing addresses, emails, phone numbers and contact preferences. At times individuals will also be contacted to ensure the data held about them is accurate.

When notified of inaccurate data by an individual, rectification will occur within one month of the date of notification by the Data Protection Officer.

For information on the current Data Protection Officer for SCT speak to the CEO.

2.6. Not be held longer than necessary (Data Suppression)

All individuals from whom SCT collects and processes personal data have the 'right to be forgotten'. This means that upon request by the individual, personal data, except data required by law to be retained, will be supressed immediately. The right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

Individuals will be informed of their right to object at the point of first communication for direct marketing and in SCT's privacy notice. One-step opt outs will also be provided for all marketing materials.

Personal data will not be held for any longer than is necessary to fulfil the purpose for which it was given. Personal data will be held for the length of time specified below based on purpose, unless there is a reason for suppression before these dates:

Individual Type	Suppression information	Data retained
Donors	2 years from last donation date	Full name, postcode (street name for Irish and ROW donors), payment information
Sponsors	2 years from last donation date	Full name, postcode (street name for Irish and ROW donors), payment information
Sponsored Children	Immediately upon leaving sponsorship programme	Full name, nickname, project
Beneficiaries	Once the become unviable for fundraising purposes	Full name, nickname, project

Contractors	Once SCT business with them has concluded unless required by law	Name, postcode
Enquires	Once the lead becomes non-viable	Name, postcode
Leads	Once the lead becomes non-viable	Name, postcode
Staff	Immediately upon leaving	Data required by law

Personal data reaching these milestones will be suppressed, not fully deleted, in accordance to data protection act regulations for charities (for more information on suppression (See Section 10).

The data controller is responsible for ensuring that all computer and print data files are regularly purged and that personal data is not held for longer than detailed above. This includes the suppression of data if there is a need to retain non-personal data.

2.7. Be processed in accordance with the rights of data subjects

Under DPA and GDPR legislation, individuals are afforded the following rights when their personal data is processed:

- Right of access to a copy of the information comprised in their personal data (see Section 13);
- Right to prevent processing for direct marketing (see Section 10); and
- Right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed (see Section 10);

SCT will adhere to all of these rights as laid out further in this policy.

2.8. Be subject to appropriate security measures

SCT will take all appropriate security measures to guard against unauthorised access to, or alteration, disclosure or destruction of, personal data. To do this SCT will:

- Store all paper files containing personal data in locked cabinets with access granted to staff on a 'need to know' basis;
- Restrict access to central IT servers to a secure location and a limited number of staff. Non-authorised staff will not have access to this server. Furthermore, any contractors will be required to sign data protection agreements before accessing the servers;
- Restrict access to any personal data within SCT to authorised staff on a 'need to know' basis as decided upon by SCT;
- Ensure that access to all computer systems are password protected with other authentication factors as appropriate due to the sensitivity of the data;
- Keep hidden information on computer screens and manual files from callers to the SCT offices;
- Back up all computer held data on a server managed by Digital Sheep;

- Train all staff in data protection as outlined in the section 'Staff Training'. The Data Protection Officer and Child Protection Officer will be responsible for ensuring that staff follow the data protection policies;
- Shred all waste paper containing any personal data; and
- Instruct the Data Protection Officer to carry out a bi-annual review of data protection measures and practices.

2.8.1. IT Security

To ensure that personal details are protected the following information technology procedures will be put in place:

2.8.2. Boundary firewalls and internet gateways

SCT has two layers of firewalls between our computers, servers and the internet. Both firewalls are configured to only allow the minimum of open ports to allow for email reception and web browsing.

2.8.3. Secure configuration

All core software used by SCT has recently been updated to the latest versions of Microsoft's Windows and Office software. Other software is kept up to date using rolling subscriptions.

2.8.4. Access control

Access to data is restricted to users and sources trusted by SCT. Only staff and volunteers have access to SCT's computer systems and each user has a unique username and password. An administrator account exists for the installation of software and computer maintenance, whose access is limited to the CEO and Accounts Assistant.

Access to Wi-Fi and other computer systems are limited by password. These passwords are changed immediately upon the departure or long absence of any staff or volunteers.

2.8.5. Malware protection

Malware and anti-virus protection is installed on the server and on each workstation used. Emails are scanned for malicious content before they hit the SCT network. Outgoing emails are also scanned for malicious content.

2.8.6. Patch management and software updates

Computer equipment and software need regular maintenance to keep it running smoothly and to fix any security vulnerabilities. Security software such as anti-virus and anti-malware needs regular updates in order to continue to provide adequate protection.

SCT persons must keep their software up-to-date by checking regularly for updates and applying them. Most software can be set to update automatically. If a system is a few years old, the relevant SCT person should review the protection he/she has in place to make sure that it is still adequate.

2.8.7. Remote Access

Remote access to the shared T: drive is available to staff at SCT, however only from devices that have been configured by the SCT IT team. These are forced to have secure passwords. Any repeated attempt to gain entry flags an alert to the IT team and the account can be monitored.

Personal data is only stored on the SCT server and the SCT Salesforce cloud database.

When personal data is accessed remotely from a personal device the following policies must be adhered to in order to prevent the loss, theft or destruction of personal data.

- Use a strong password to secure devices;
- Ensure access to the device is locked if an incorrect password is input more than three times;
- Ensure the device automatically locks after it has been inactive for a period of no longer than 15 minutes;
- Personal data should never be stored on the device. Devices should be used to access secure cloud servers only;
- Do not save Salesforce passwords on the device as in the event the device is stolen all personal data will be accessible; and
- Register device with Mobile Device Management software which allows you to remotely access and delete data from your device in the event of loss or theft.

All traffic to access personal data will be accessed through a HTTPS connection when using an untrusted connection (i.e. a coffee shop or hotel Wi-Fi).

In the event of the loss or theft of the device, staff will be required to contact the Data Protection Officer immediately, who will then assess the threat. All passwords relating to the access of personal data such as work email and Salesforce must be changed immediately. In the event of a computer or device (e.g. phone, tablet) being lost, which has been configured for remote access to the shared T: drive, it can be remotely wiped and SCT data removed from it.

2.8.8. Data Backup

Backups are taken three times a day internally and backed up off-site once per day.

2.9. Not to be transferred outside the EEA unless specific conditions have been met

SCT will not transfer data outside of the EEA unless specifically necessary for the administration of the Child Sponsorship Programme. Data will only be transferred if the following conditions are met:

- Consent is received from the individual; and
- Data transfer is necessary for the performance of the contract between SCT and the individual.

Only personal data required for the relationship between the child sponsor and their sponsor child will be shared with projects in Thailand. This information consists of *ONLY* the sponsor's full name.

When transferring data outside of the EEA, SCT will strive to ensure the most stringent data protection measures are taken. Information is sent via a secure server and projects in Thailand are required to sign Contractual Clauses based on EU Model Contractual Clauses which outline data protection measures projects will take to ensure sponsors data is protected in accordance with EU data protection regulations.

2.10. Be provided to individuals upon their request

Upon written request, SCT will provide any individual with the following information:

- A copy of the data that is kept about him or her;
- The purposes for which their data is retained; and
- The source of the data.

In order to do so, the following information will be required before access to SCT data is granted:

- Full name and contact details of the person making the request;
- Requester's relationship with SCT;
- Time period in which relationship occurred;
- Signed letter of consent from a third-party to access a donors' data if applicable; and
- Signed third party data protection and confidentiality agreement.

We may also require proof of identity before access is granted. Two of the following forms of ID will be required:

- Birth Certificate;
- Passport;
- Driver's license; and
- Bill or bank statement.

The Data Protection Officer is responsible for correcting or erasing any inaccurate data and removing personal data off direct marketing or mailing lists upon request.

All personal data must be supplied to the individual within 30 days of receiving the written request.

All requests for personal data should be addressed to or passed on to the Data Protection Officer, who will be responsible for processing the request. SCT may bring disciplinary proceedings against an SCT person who is suspected of or found to have disclosed personal data and/or infringed any other part of this policy. Sanctions for any unauthorised disclosure of personal data to a third party may result in immediate dismissal as determined by the terms of employment.

Any unauthorised disclosure of personal data may result in in civil claims being made against SCT and fines being imposed.

3. Responsibilities of SCT

Overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of SCT, this is the Board of Trustees.

The governing body delegates tasks to the CEO and the Data Protection Officer. The CEO and Data Protection Officer are responsible for:

- understanding and communicating obligations under the legislation;
- identifying potential problem areas or risks; and
- producing clear and effective procedures.

All SCT persons who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles. Breach of this policy may result in disciplinary actions.

Third party providers are required to sign a Third Party Confidentiality and Data Protection Agreement before commencing any work for SCT. All relevant data protection procedures are provided in the agreement. Third parties can also request a full copy of the Data Protection Policy for clarification.

4. Policy Implementation

To meet our responsibilities SCT persons will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely; and
- Ensure the rights people have in relation to their personal data can be exercised.

SCT will ensure that:

- Everyone managing and handling personal information is trained to do so by a qualified individual;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows how to access information on the policy and procedures;
- All direct marketing will provide supporters with an opt-out option and a suppression list will be maintained; and
- Any disclosure of personal data will be in line with SCT's procedures.

Queries about handling personal information will be dealt with swiftly and politely.

5. Child Protection

In conjunction with our Safe Guarding Policy, beneficiaries will have their identities protected to ensure they cannot be located or contacted in any capacity outside of SCT facilitation.

5.1. Child Safeguarding

- SCT will never reveal a beneficiary's full name; date of birth; home address (or address of the organisation where the beneficiary is resident); name or location of schools, hospitals, day-care centres or other facilities used by the beneficiary;
- SCT will use nicknames and/or pseudonyms to refer to the beneficiary, to retain anonymity;
- SCT will only reveal the location of the beneficiary by province (regional area) and will not disclose identifying features of projects or programmes used by the beneficiary. This should be observed in all communications with particular attention to social media postings;
- SCT will never share a beneficiary's private or personal contact details i.e. email address, social media handle, phone number, home address etc.;
- SCT will not disclose personal details that impeach upon the privacy, rights and dignity of the beneficiary, for example, HIV/AIDs status; sexual orientation; pregnancy; history of severe neglect, rape or sexual abuse; substance addiction; mental health status; criminal convictions; gender orientation or any other personal information deemed likely to threaten the beneficiary's confidentiality, privacy or cause distress or discrimination, and take appropriate steps to keep such information confidential in secure environments;
- All beneficiaries enrolled in the Child Sponsorship Scheme, or featuring in SCT appeals, campaigns or marketing activities will be briefed by programme coordinators about the nature of the Child Sponsorship Scheme and their involvement;
- Beneficiaries over the age of 16 will be asked to give consent to featuring in the charity's publications. They must read and sign a consent form, explaining how their data and images may be used and giving SCT permission to use this information in fundraising activity and the Child Sponsorship Scheme;
- Beneficiaries between the ages of 12 – 16 will co-sign a consent form with a parent or legal guardian;
- For beneficiaries under the age of 12, a parent or legal guardian will be asked to give consent on behalf of the child; and
- In all cases where beneficiaries over 16 have an intellectual disability or are considered unable to understand the terms of consent, a parent or legal guardian must give consent on their behalf.

5.2. Use of images

- Images and stories should only be used in the intended context and for the purpose for which consent was obtained;
- In photographs, beneficiaries will be appropriately and modestly dressed, with outer clothing garments covering their torso (i.e. no swimwear). Photographs will be dignified and age- and culture-appropriate; and
- SCT will not use images of beneficiaries that may cause embarrassment, distress, indignity or upset.

5.3. Donor/beneficiary relationship management

- SCT will receive, process and distribute all communications between sponsor and sponsee or donor and beneficiary. This includes the exchange of gifts, messages, cards and letters. The SCT administration team will ensure that all communications

are, to the extent appropriate given the terms of this policy, censored, confidential and uphold commitment to this safeguarding policy and procedures;
- SCT will not facilitate, in any capacity, unaccompanied individual visits to or from beneficiaries;
- SCT will not facilitate private financial transactions to individual beneficiaries to private bank accounts; and
- Breach of the above procedures by donors or sponsors could result in the termination of sponsorship.

6. Training

Training and awareness raising about the relevant data protection legislation and how it is followed in this organisation will take the following forms:

- On induction: Any SCT persons will undergo an initial training consisting of a review of SCT's data protection policies and the implications upon their role; and
- General training/ awareness raising: The SCT's data protection policies will be available in print and on the shared drive which will be available to all SCT persons. A copy of the policies will be provided to each Trustee. All staff will be required to attend a yearly data protection training which will include any relevant changes to data protection legislation and SCT's Data Protection Policies.

7. Breaches of Personal Data

In the event of a breach of the personal data held by SCT, steps will be taken immediately to close or contain the breach then mitigate any risks arising from the data breach. Individuals affected by the data breach will be informed by the Data Protection Officer within 72 hours from when the breach is discovered.

8. Queries

Queries about handling personal information will be dealt with swiftly. We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the timeframe required by the relevant legislation from receiving the written request. SCT's CEO should also be contacted in general for any doubts and uncertainties in dealing with any third party request.

This policy will be reviewed at intervals of 1 year to ensure it remains up to date and compliant with relevant legislation.

Reviewed pro bono by:

goodcorporation