Empower with an education to prevent sex trafficking

CONFIDENTIALITY POLICY

Document Control	
Document Title	Confidentiality Policy
Document ID	HR-003
Version	V3.0
Status	Approved
Author	Sarah Rogers, Country Director
Review Date	23 April 2026
Reviewer	Nicky Mih, Managing Director
Approval Authority	Board
Approval	Merewyn Foran, Board Chair
Approval Date	5 May 2026
Board Resolution	Board Meeting 50, May 2026
Effective Date	May 2026
Creation Date	September 2017
Last Review	May 2021
Next Review	Quarter 3, 2028-2029

ACN 143 986 074
www.freetoshine.org
info@freetoshine.org

CONFIDENTIALITY POLICY

CONTENTS

1. PURPOSE

This Confidentiality Policy establishes Free to Shine's (FTS) commitment to protecting the privacy, dignity, and safety of all individuals associated with our organisation, including clients, employees, volunteers, donors, partners, and other stakeholders.

It helps us protect sensitive information, maintain trust and safeguard organisational reputation and credibility. It sets out the principles that guide how FTS manages confidential information and is in alignment with the ACFID Code of Conduct, the Australian Privacy Principles (APPs) under the Privacy Act 1988, and relevant Cambodian legal requirements.

Respecting confidentiality is a fundamental responsibility for all FTS employees, as it is essential to safeguarding clients, their families, and the integrity of the organisation. Employees may access sensitive or private information as part of the requirements of their role, including personal details of children, families, and colleagues, as well as case notes, assessments, and information about child protection or welfare concerns. All such information collected, accessed, or generated through work (paid or unpaid) for FTS must be treated as strictly confidential and handled in accordance with this policy.

This Confidentiality policy should be read in conjunction with FTS's public Privacy Policy.

2. SCOPE

This policy applies to all:

- Employees, including full-time, part-time, and casual
- Board members
- Volunteers, students, and interns
- Consultants and contractors
- Partners and donors

3. RESPONSIBLE PARTIES

The Country Director and Operations Manager are responsible for ensuring that this Confidentiality Policy is included in all induction and training processes, and that all employees understand it and formally agree to comply with it.

4. DEFINITIONS

Confidential information is any non-public information that a person accesses through their work with FTS and that could reasonably be expected to be kept private or protected. It may relate to individuals (such as clients, children, family members, employees, volunteers, donors) or to the organisation and its partners. Confidential information at FTS includes, but is not limited to:

Category	Examples
Personal information	Names, contact details, dates of birth, identification documents, photographs, donation and donor data.
Sensitive information	Health and disability information, trauma or abuse history, family circumstances, religious or ethnic background, bank account details., whistleblower complaints.
Child-related information	Case files, assessments, school and case management records, protection concerns, images or stories about children.
Organisational information	Strategic and program plans, financial data, donor information, internal reports and documents, board papers and discussions, legal matters.
Partner information	Partnership agreements, financial arrangements, joint program data, and other non-public information shared by partners.

Information does not stop being confidential because it is stored digitally or discussed verbally; the same duty of confidentiality applies regardless of format or location.

5. POLICY STATEMENT AND KEY PRINCIPLES

FTS is committed to protecting the confidentiality of personal and sensitive information, respecting the privacy, dignity, and rights of all stakeholders, and handling information ethically and in accordance with legal obligations. We aim to maintain trust through responsible information management and to safeguard children and vulnerable individuals through appropriate information controls.

To achieve this, FTS will:

- Respect the dignity, values, culture, and rights of all individuals when collecting, using, and sharing information.
- Obtain free, prior, and informed consent before collecting, using, or disclosing personal information, except where law or serious safety concerns require otherwise.
- Client information: Collect and retain only the minimum information necessary for program delivery, organisational strategy delivery, legal and regulatory obligations, whistleblowing and safeguarding.
- Apply heightened protections to information relating to children and vulnerable people, consistent with our Child Protection Policy and Protection from Sexual Exploitation, Abuse and Harassment (PSEAH) Policy.
- Maintain information security through appropriate technical, physical, and organisational safeguards.
- Ensure sensitive information is only shared on an as-needs basis.

6. INFORMATION HANDLING STANDARDS

These internal standards operate in conjunction with FTS's public Privacy Policy, which explains what personal information FTS collects, why we collect it, and how we use, store, disclose, and protect it, including when information is stored in or accessed from systems located outside Australia, and how individuals can exercise their rights.

6.1 Collection

- Collect personal information lawfully, fairly, and only where necessary for FTS's work and legal obligations.
- Inform individuals about why information is collected, how it will be used and stored, who may access it, and their consent options.

6.2 Storage and Security

- Store information securely in physical and digital systems, with access restricted on a need-to-know basis.
- Apply appropriate technical and organisational security measures in line with internal information security procedures.

6.3 Use and Disclosure

- Use information only for the purpose for which it was collected, unless the individual has consented to another use, a law requires or permits it, or it is necessary to prevent or reduce a serious threat to life, health, or safety.
- Disclose information to third parties only where there is a clear consent, legal basis, or safeguarding need, and subject to appropriate confidentiality obligations.

6.4 Access, Correction, and Consent

- Individuals have the right to request access to their personal information and to request correction of inaccurate, incomplete, or out-of-date information, in line with applicable laws.
- The Operations Manager will manage access, correction, and consent-related requests in accordance with this policy, the Privacy Policy, privacy legislation, and FTS procedures.

6.5 Retention and Destruction

- Retain information only for as long as it is needed for its purpose or to meet legal, contractual, or donor requirements, including minimum periods set in relevant laws and internal schedules.
- When information is no longer required, securely destroy or de-identify it using methods specified in FTS's privacy procedures.

7. CHILD PROTECTION AND COMMUNICATIONS

Children's information receives heightened protection, and no identifying details that could enable the location or contact of a child will be included.

Images and stories of children will be used only with appropriate guardian consent, child's views where appropriate, and in line with FTS's Child Protection and Communications policies.

Case information involving abuse or protection concerns is shared in accordance with the Child Protection Policy and legal obligations.

8. USE OF INFORMATION TECHNOLOGY SYSTEMS AND THIRD-PARTY SERVICES

FTS only collects, stores and processes confidential information (including client, case, donor, employee and partner information) in approved information systems and services that provide appropriate safeguards for privacy, security and confidentiality. Employees, volunteers and contractors must not use personal email accounts or unapproved applications to record, transmit or store confidential information.

FTS uses secure cloud-based systems, including the OSCaR case management system (hosted in Cambodia) and Google Workspace (Google Drive), to store and manage personal information. These systems may be accessed by authorised FTS staff in Australia and Cambodia. Personal information held in these systems may therefore be stored on servers located outside Australia.

FTS maintains effective control over personal information stored in these systems and takes reasonable steps to ensure that service providers protect personal information in a way that is consistent with the Australian Privacy Principles, including through contractual terms, technical and organisational security measures, access controls, and restrictions on secondary use and onward disclosure.

Before any new system, application or service is adopted at FTS, it must be assessed and approved through the organisation's information security and privacy due-diligence process, including consideration of data protection measures, data location, access controls and contractual confidentiality and privacy obligations. All third-party providers that access or store confidential information must be bound by suitable agreements and meet relevant legal and regulatory requirements; if they cannot meet these standards, they must not be used for confidential information.

9. OBLIGATIONS AND BREACHES

All employees, board members, volunteers, students, interns, consultants, and contractors must protect confidential information at FTS, including information about children and families, colleagues, donors, partners, and the organisation itself.

Confidential information must not be disclosed to anyone outside FTS, including family or friends, unless clearly authorised, required by law, or permitted under this policy (for example, to prevent harm in a safeguarding situation).

Confidential information may only be accessed and used for legitimate FTS work purposes, and never for personal benefit or unrelated activities. FTS must always be able to justify any decision to share confidential information in line with this policy and applicable laws.

9.1 Obligations of employees

All employees must:

- Sign a confidentiality agreement and complete required confidentiality and privacy training
- Use and share confidential information only where it is necessary for their role and on a need-to-know basis with authorised colleagues
- Keep information secure in accordance with FTS policies and procedures
- Refrain from discussing confidential information in public or unsecured places, including on phones where they may be overheard
- Seek guidance from their line manager or the Operations Manager if unsure whether information can be shared
- Promptly report any suspected or actual breaches
- Return all confidential information to FTS at the end of employment or engagement, or earlier as directed by a line manager or Operations Manager
- Continue to respect confidentiality after their employment or engagement with FTS ends

9.2 Breaches of confidentiality

A breach of confidentiality occurs when confidential information is accessed, used, shared, or managed in a way that is inconsistent with this policy, whether intentional or accidental. All suspected or actual breaches must be reported promptly to a line manager or the Operations Manager.

Breaches will be treated as serious misconduct and may result in disciplinary action, up to and including termination of employment or engagement, and reporting to relevant authorities where required by law or necessary to protect a child or vulnerable person.

10. EXCEPTIONS

Confidentiality may be breached without consent when required by law (such as court orders or mandatory reporting), when necessary to prevent serious harm to a child or vulnerable individual, to prevent a serious threat to life, health, or safety, or where there is evidence of serious criminal activity. Only the minimum necessary information will be disclosed, and decisions will be documented, approved by management where possible, and communicated to the individual concerned where it is safe and appropriate to do so.

11. THIRD-PARTY INFORMATION SHARING

When FTS shares confidential information with third parties (such as partner organisations, service providers, or government agencies), we will:

- Use written agreements that clearly set out the purpose of sharing, the types of information to be shared, security and confidentiality obligations, retention and disposal requirements, and limits on further disclosure.
- Share information only with organisations that have appropriate safeguards and are bound by obligations that are consistent with FTS's legal and policy requirements.
- Inform individuals when their personal information is likely to be transferred to another country, obtain consent where required, and ensure any cross-border disclosure is necessary, lawful, and limited to the minimum information needed.
- Ensure that any disclosure of personal information is for the primary purpose for which it was collected, or is otherwise permitted by law or valid informed consent.

12. TRAINING

All employees, volunteers, and board members will receive confidentiality and privacy training as part of their induction, with periodic refresher training to maintain awareness of their obligations under this policy. Relevant employees whose roles involve handling sensitive information will receive additional role-specific guidance where required.

13. COMPLIANCE, MONITORING AND LEARNING

FTS monitors compliance with this policy through line management supervision, training records, and periodic reviews or audits of information-handling practices, including checks of access controls, case records, and confidentiality and privacy procedures. Incidents, near misses, and complaints relating to privacy or confidentiality are documented, reviewed, and used to strengthen systems, procedures, and practice.

All suspected or actual breaches of confidentiality must be reported promptly in accordance with section 9.2 (Breaches of confidentiality) and managed under FTS's disciplinary and incident-management procedures, including reporting to regulators or funders where required. Any privacy or confidentiality breaches will be recorded, investigated, and the outcomes used to improve controls, guidance, and staff training.

Individuals may raise concerns or make complaints about privacy or confidentiality by contacting the Operations Manager or by using FTS's Complaints and Feedback Policy and procedure. Further information about privacy rights and how to make a complaint is available on FTS's website and, where relevant, through the Office of the Australian Information Commissioner.

Where personal information is stored in or accessed through cloud services or systems located overseas (including the OSCaR case management system and Google Workspace), FTS takes reasonable steps to ensure those service providers handle personal information in a manner consistent with the Australian Privacy Principles, and FTS remains accountable for that handling under the Privacy Act 1988 (Cth).

14. POLICY REVIEW

This policy will be reviewed at least every three years, or sooner if required by changes in legislation, donor or regulatory requirements, significant breaches or incidents, audit findings, or FTS's operational needs.

15. RELATED POLICIES AND LEGAL FRAMEWORK

This Confidentiality Policy should be read alongside:

- Child Protection Policy
- Code of Conduct
- Complaints and Feedback Policy
- Privacy Policy
- Whistleblower Policy
- Employment Policy
- PSEAH Policy
- Communications Policy

These documents together set out FTS's expectations for safe, ethical, and lawful conduct, including how concerns about privacy or confidentiality can be raised and addressed.

Legal and regulatory framework

This policy is informed by and intended to align with:

- ACFID Code of Conduct (including Quality Principle 7 and Principles 6.2.1 and 6.2.2)
- Privacy Act 1988 (Australia) and the Australian Privacy Principles
- ACNC External Conduct Standards
- United Nations Convention on the Rights of the Child (UNCRC)
- Cambodian Constitution and other relevant Cambodian laws relating to privacy and data protection

REVISION LOG

Version	Date	Summary of Changes	Author
1	September 2017	Initial policy release	Nicky Mih, Managing Director
2	May 2021	Review, update and rewrite	Nicky Mih, Managing Director
3	February 2026	Major review and rewrite	Sarah Rogers, Country Director

ATTACHMENT 1: CONFIDENTIALITY AND PRIVACY AGREEMENT

Free To Shine

Confidentiality and Privacy Declaration

Name: _____

Position/Role: _____

Start Date: _____

1. Purpose

This declaration confirms that you have read, understood, and agree to comply with Free to Shine's Confidentiality Policy and Privacy Policy, as well as your obligations under relevant Australian and Cambodian laws.

2. Acknowledgement of confidentiality obligations

I acknowledge and agree that:

a) Confidential information
During my work (paid or unpaid) with Free to Shine (FTS), I may access confidential information relating to clients (including children and their families), colleagues, donors, partners, and the organisation itself. This includes personal information, sensitive information, child-related information, organisational information, and partner information as defined in the Confidentiality Policy.

b) Duty of confidentiality
I will treat all confidential information as strictly private and will:

- Only access confidential information where it is necessary for my role
- Use confidential information only for legitimate FTS work purposes, never for personal benefit or unrelated activities
- Share confidential information internally only on a need-to-know basis with authorised colleagues
- Not disclose confidential information to anyone outside FTS (including family, friends, or the public) unless clearly authorised, required by law, or permitted under the Confidentiality Policy (for example, to prevent harm in a safeguarding situation)
- Keep information secure in accordance with FTS policies and procedures
- Avoid discussing confidential information in public or unsecured places where I may be overheard
- Return all confidential information to FTS at the end of employment or engagement, or earlier as directed by a line manager or Operations Manager

c) Children's information
I understand that children's information requires heightened protection and that I must never:

- Use full names alongside photographs of children
- Include identifying details that could enable location or contact of a child
- Share images, stories, or information about children without appropriate consent and authorisation from management

d) Seeking guidance
If I am unsure whether information can be shared or how to handle a confidentiality matter, I will seek guidance from my line manager or the Operations Manager (Privacy Officer) before taking action.

e) Reporting breaches
I will promptly report any suspected or actual breaches of confidentiality to my line manager or the Operations Manager.

f) Continuing obligation
I understand that my duty of confidentiality continues after my employment or engagement with FTS ends, and I will continue to protect confidential information I accessed during my time with FTS.

3. Consequences of breaches

I understand that breaches of confidentiality will be treated as serious misconduct and may result in disciplinary action, up to and including termination of my employment or engagement, and reporting to relevant authorities where required by law or necessary to protect a child or vulnerable person.

4. Policies received and read

I confirm that I have received, read, and understood the following policies:

- ☐ Confidentiality Policy
- ☐ Privacy Policy
- ☐ Child Protection Policy
- ☐ PSEAH Policy
- ☐ Code of Conduct
- ☐ Communications Policy

5. Declaration

I declare that I will comply with the Free To Shine Confidentiality Policy, Privacy Policy, and all related policies and procedures, and that I will uphold the privacy, dignity, and safety of all individuals whose information I may access.

Signature: _____

Print Name: _____

Date: _____

Witnessed by (Manager/HR): _____

Signature: _____

Date: _____

For office use:
☐ Original filed in personnel file
☐ Copy provided to employee
☐ Recorded in HR system