

CONFIDENTIALITY & INFORMATION HANDLING POLICY

Shield and Rebuild Charity LTD

Document	Confidentiality & Information Handling Policy
Version	2.0
Draft date	12 September 2026
Status	Draft for formal Board adoption
Policy owner	Board / Responsible People
Review cycle	At least annually and after material legal, operational or safeguarding change
Next scheduled review	September 2027

Important status

This document is an updated governance-policy draft prepared for Shield and Rebuild. It should be formally considered and adopted by the Board/Responsible People before being represented as an approved organisational policy. It is not an ACNC-approved document and is not legal advice.

1. PURPOSE

To protect confidential, personal, security-sensitive and organisational information from unauthorised access, use or disclosure while allowing necessary information sharing for safe, lawful and effective charitable operations.

2. SCOPE

This policy applies to the Board/Responsible People, employees, volunteers, contractors, consultants, students, partner organisations and any person acting for or representing Shield and Rebuild. Contractual arrangements should require relevant third parties to meet equivalent standards where appropriate.

3. WHAT IS CONFIDENTIAL

Confidential information includes applicant and beneficiary identities; addresses and contact details; referral narratives; police and court information; criminal-history and citizenship evidence; health or safeguarding information; security assessments, floorplans, CCTV positions, alarm/access details and codes; complaint and investigation records; donor and personnel information; contracts, pricing, governance papers and other non-public organisational information.

4. NEED-TO-KNOW RULE

Personnel may access or share confidential information only where reasonably required for their authorised role. Curiosity, convenience or personal relationships are not valid reasons for access. Where a contractor only needs a site address and approved work scope, unrelated referral or trauma information should not be provided.

5. COLLECTION AND DISCUSSION

Do not seek unnecessary sensitive details. Avoid discussing cases in public areas, vehicles where others can hear, social media, personal messaging groups or with family/friends. Use approved organisational systems where available.

6. SECURITY INFORMATION

Security designs, vulnerabilities, access credentials, camera locations and similar information can create direct physical risk if mishandled. Share them only with authorised persons and never publish them without a documented reason and authority.

7. SAFEGUARDING AND COMPLAINT INFORMATION

Allegations and reports must be handled discreetly, but confidentiality is not absolute. Information may need to be shared to protect a person, obtain emergency help, report suspected crime, comply with safeguarding/reporting obligations, investigate fairly or meet a lawful direction.

8. DIGITAL AND PHYSICAL HANDLING

Use strong authentication, appropriate access controls and secure storage. Do not leave forms, devices or case notes unattended in public. Verify recipients before sending sensitive material. Lost devices, misdirected emails, exposed files or suspected unauthorised access must be reported immediately.

9. CONTRACTORS, PARTNERS AND VOLUNTEERS

Provide only the information required for the task. Relevant agreements, onboarding or directions should include confidentiality, privacy, safeguarding, information-security and return/destruction requirements proportionate to the work.

10. MEDIA, PHOTOGRAPHY AND CASE STUDIES

Do not identify or photograph beneficiaries, children, properties or security installations for publicity without appropriate documented authority and a risk assessment. Consent should be informed, voluntary and specific; declining publicity must not affect access to assistance.

11. END OF ENGAGEMENT

Confidentiality obligations continue after employment, volunteering, contracting or Board service ends. Organisational records and devices must be returned, transferred or securely destroyed as directed.

12. BREACHES

Suspected confidentiality breaches must be reported immediately. Shield and Rebuild will assess safety, privacy, legal, contractual and reputational consequences; contain the breach; preserve evidence; notify affected people or authorities where required; and take proportionate corrective action.

DOCUMENT CONTROL & REVIEW

The Board/Responsible People will review this policy at least annually and sooner following a serious incident, complaint trend, material change to services, legislative change, regulatory guidance, or identified control weakness. Superseded versions should be retained in accordance with the organisation's recordkeeping requirements.

Website: www.shieldandrebuild.com