- **Burmese Community Development Collaboration (BCDC)**

PRIVACY POLICY

Version 2.0
Reviewed on May 2027

BCDC
BURMESE COMMUNITY
DEVELOPMENT COLLABORATION

Table of Contents

1. Introduction

The Burmese Community Development Collaboration (BCDC) is committed to protecting the privacy, dignity, confidentiality, and personal information of all individuals who engage with the organisation through its programs, services, partnerships, community activities, and operational processes.

BCDC recognises that the organisation may collect, store, use, manage, and protect personal and sensitive information relating to:

- Refugees and displaced persons;
- Community members and beneficiaries;
- Children and vulnerable individuals;
- Staff and volunteers;
- Partner organisations and stakeholders;
- Donors, supporters, and service users.

The organisation further recognises that many individuals associated with BCDC may come from vulnerable, conflict-affected, displacement, or high-risk backgrounds where privacy and confidentiality are critically important for safety, dignity, safeguarding, and protection.

This Privacy Policy establishes the principles, standards, and procedures that guide how BCDC collects, manages, stores, uses, protects, and discloses personal information in accordance with:

- Australian Privacy Principles (APPs);
- Relevant Australian privacy laws;
- Safeguarding obligations;
- ACFID Code of Conduct requirements;
- Ethical and humanitarian principles.

2. Purpose of the Policy

The purpose of this policy is to:

- Protect the privacy and confidentiality of individuals associated with BCDC;
- Ensure responsible and lawful collection and handling of personal information;
- Promote safe and ethical information management practices;
- Support safeguarding and protection obligations;
- Prevent unauthorised access, misuse, disclosure, or loss of information;
- Ensure transparency regarding how personal information is managed;
- Strengthen trust, accountability, and organisational integrity.

This policy also seeks to ensure that individuals understand:

- What information may be collected;
- Why information is collected;
- How information may be used or shared;
- How information is protected;
- What rights individuals have regarding their personal information.

3. Organisational Commitment to Privacy and Confidentiality

BCDC is committed to maintaining respectful, ethical, secure, and safeguarding-informed privacy practices across all organisational activities.

The organisation is committed to:

- Respecting the dignity and privacy of all individuals;
- Protecting confidential and sensitive information;
- Maintaining secure information management systems;
- Supporting informed consent processes;
- Preventing unauthorised disclosure or misuse of information;
- Protecting refugee and vulnerable community confidentiality;
- Applying safeguarding principles to information management;
- Managing information responsibly and transparently.

BCDC recognises that breaches of privacy or confidentiality may:

- Place individuals at risk of harm;
- Affect safeguarding and protection outcomes;
- Damage trust and community relationships;
- Create legal and reputational risks;
- Undermine humanitarian and community support efforts.

4. Scope and Application

This policy applies to:

- Board members;
- Employees and staff;
- Volunteers and interns;
- Contractors and consultants;
- Partner organisations and representatives;
- Community workers and facilitators;
- Individuals engaged in BCDC-supported activities.

This policy applies to:

- Physical records and paper documents;
- Digital and electronic information;
- Email and online communications;
- Databases and storage systems;
- Audio, video, and photographic materials;
- Website and online engagement platforms;
- Social media and digital communication activities.

The policy applies across all BCDC operational, humanitarian, safeguarding, and community engagement activities conducted within Australia or internationally.

5. Legal and Regulatory Framework

BCDC is committed to managing personal information in accordance with applicable legal, ethical, and sector obligations.

This policy is informed by:

- Australian Privacy Principles (APPs);
- Privacy Act 1988 (Cth);
- ACFID Code of Conduct requirements;
- Safeguarding and PSEAH obligations;
- Child protection obligations;
- Relevant confidentiality and record-keeping requirements;
- Ethical humanitarian and community development principles.

Where safeguarding, child protection, or legal obligations require mandatory reporting or disclosure, BCDC may disclose information in accordance with applicable laws and organisational procedures.

6. Definitions

For the purpose of this policy, the following definitions apply.

Personal Information
Personal information refers to information or an opinion about an identified individual or an individual who can reasonably be identified. This may include names, addresses, contact details, identification records, photographs, case information, or other personal details collected through BCDC activities or services.

Sensitive Information
Sensitive information refers to information requiring a higher level of confidentiality and protection due to its personal or vulnerable nature. This may include information relating to health, ethnicity, refugee status, safeguarding concerns, trauma experiences, disability, legal matters, or child protection concerns.

Confidential Information
Confidential information refers to information that must be protected from unauthorised access, disclosure, misuse, or distribution. This includes personal information, safeguarding records, refugee case information, financial information, investigation records, and organisationally sensitive materials.

Consent
Consent refers to voluntary, informed, and clear agreement provided by an individual for BCDC to collect, use, store, disclose, photograph, record, or otherwise manage their personal information. Consent may be written, verbal, digital, or otherwise appropriately documented.

Safeguarding Information
Safeguarding information refers to any information relating to child protection, PSEAH concerns, vulnerable individuals, incidents of harm, exploitation, abuse, neglect, or safeguarding investigations. Such information requires strict confidentiality and protection measures.

Data Breach
A data breach refers to unauthorised access, disclosure, misuse, loss, alteration, destruction, or release of personal or confidential information. Data breaches may occur through physical, electronic, verbal, or online information handling failures.

Refugee or Client Information
Refugee or client information refers to personal, case-related, or protection-related information collected from refugees, displaced persons, asylum seekers, beneficiaries, or community members accessing BCDC programs or services. This information may involve highly sensitive personal or protection-related circumstances.

Media Consent
Media consent refers to permission granted by an individual for BCDC to use photographs, videos, audio recordings, stories, testimonials, or other media materials for organisational, safeguarding, communication, advocacy, reporting, or promotional purposes.

7. Types of Personal Information Collected

BCDC may collect personal and sensitive information necessary to support organisational operations, humanitarian activities, safeguarding responsibilities, service delivery, community engagement, and legal or compliance obligations.

The types of information collected may include:

- Full names and identification details;
- Contact information;
- Emergency contact information;
- Demographic information;
- Refugee or migration-related information;
- Case management or support information;
- Safeguarding and protection-related information;
- Health or wellbeing information where necessary;
- Employment, volunteer, or training records;
- Financial or payment-related information where required;
- Photographs, audio recordings, or video materials;
- Digital communication or online engagement information.

BCDC recognises that some individuals associated with the organisation may come from vulnerable, displacement, or conflict-affected backgrounds. Accordingly, sensitive information must be handled carefully, respectfully, and confidentially.

The organisation will seek to collect only information that is:

- Relevant;
- Necessary;
- Lawful;
- Appropriate for operational or safeguarding purposes.

8. Methods of Information Collection

BCDC may collect personal information through lawful, fair, and transparent methods consistent with organisational and safeguarding obligations.

Information may be collected:

- Directly from individuals;
- Through registration or intake forms;
- During service delivery or community engagement activities;
- Through safeguarding or incident reporting processes;
- During volunteer or employment processes;
- Through surveys, interviews, assessments, or consultations;
- Through digital communication platforms;
- Through website, email, or online engagement activities;
- Through photographs, video recordings, or media activities where consent is provided.

In some circumstances, information may also be collected from:

- Parents or guardians;
- Partner organisations;
- Referral agencies;
- Service providers;
- Legal representatives;
- Publicly available sources where lawful and appropriate.

BCDC will seek to ensure that individuals understand:

- Why information is being collected;
- How information may be used;
- Whether information may be shared;
- What confidentiality protections apply.

Information collection processes should remain respectful, culturally sensitive, safeguarding-informed, and appropriate to the operational context.

9. Consent and Lawful Collection of Information

BCDC is committed to collecting personal information lawfully, fairly, transparently, and with appropriate consent wherever possible.

The organisation will seek informed consent before collecting, using, storing, sharing, photographing, recording, or publishing personal information unless:

- Legal obligations require otherwise;
- Safeguarding or protection concerns require immediate action;
- Emergency situations apply;
- Information collection is otherwise authorised by law.

Consent processes should:

- Be voluntary and informed;
- Be explained clearly and respectfully;
- Be appropriate to the individual's language and understanding;
- Consider safeguarding and vulnerability factors;
- Allow individuals to ask questions or decline participation where appropriate.

Where children or vulnerable individuals are involved, BCDC may seek consent from:

- Parents or guardians;
- Appropriate caregivers;
- Authorised representatives;
- Responsible safeguarding personnel where applicable.

BCDC recognises that individuals may withdraw consent in some circumstances. The organisation will seek to respect such requests where operationally, legally, and safeguarding-wise appropriate.

The organisation will also seek to ensure that:

- Only necessary information is collected;
- Information collection is proportionate and relevant;
- Sensitive information receives additional protection;
- Confidentiality obligations are maintained throughout the information management process.

10. Refugee, Client, and Community Confidentiality

BCDC recognises that many refugees, displaced persons, asylum seekers, vulnerable individuals, and community members may face heightened privacy, protection, and safeguarding risks.

Accordingly, the organisation is committed to maintaining strict confidentiality regarding:

- Refugee or migration-related information;
- Protection-related information;
- Safeguarding and PSEAH information;
- Personal case records;
- Health or wellbeing information;
- Legal or family-related matters;
- Sensitive community information.

BCDC understands that unauthorised disclosure of information may:

- Place individuals or families at risk;
- Affect refugee or protection processes;
- Cause emotional distress or trauma;
- Damage trust and community safety;
- Create safeguarding and security risks.

Access to refugee, client, or community information should be restricted to authorised personnel with legitimate operational, safeguarding, or legal responsibilities.

Personal information should not be:

- Shared unnecessarily;
- Published without consent;
- Discussed in inappropriate settings;
- Distributed outside approved organisational processes;
- Used in ways that may place individuals at risk of harm.

Where photographs, stories, testimonies, or case information are used for advocacy, reporting, fundraising, or communication purposes, BCDC will seek appropriate informed consent and take steps to protect dignity, safety, and confidentiality.

11. Safeguarding and Sensitive Information Protection

BCDC recognises that safeguarding and sensitive information requires a higher level of confidentiality, protection, and responsible handling due to the potential risks of harm, exploitation, discrimination, retaliation, or trauma.

Sensitive information may include:

- Child protection records;
- PSEAH-related information;
- Safeguarding reports or investigations;
- Refugee or protection-related information;
- Health or wellbeing information;
- Trauma-related disclosures;
- Legal or security-related information;
- Information relating to vulnerable individuals or communities.

BCDC is committed to:

- Protecting safeguarding and sensitive information from unauthorised access or disclosure;
- Restricting access to authorised personnel only;
- Managing safeguarding information using survivor-centred and protection-focused approaches;
- Ensuring secure storage and handling of sensitive records;
- Preventing unnecessary sharing or exposure of confidential information.

Sensitive safeguarding information should only be shared:

- On a need-to-know basis;
- For safeguarding or protection purposes;
- To comply with legal obligations;
- To prevent serious harm or risk;
- Through approved organisational processes.

Failure to appropriately protect safeguarding or sensitive information may constitute serious misconduct and may result in disciplinary or corrective action.

12. Child and Vulnerable Person Data Protection

BCDC is committed to protecting the privacy, dignity, safety, and personal information of children and vulnerable individuals engaged in organisational activities, programs, services, or community engagement processes.

Information relating to children and vulnerable individuals must be handled with particular care and sensitivity due to increased safeguarding and protection risks.

BCDC will seek to ensure that:

- Information collection involving children is appropriate and necessary;
- Consent is obtained from parents, guardians, or authorised caregivers where required;
- Child-related information is stored securely and confidentially;
- Access to child or vulnerable person records is restricted to authorised personnel;
- Personal information is not shared unnecessarily or in ways that may place individuals at risk.

Photographs, videos, stories, case studies, or personal information involving children or vulnerable individuals should not be used without appropriate consent and safeguarding consideration.

BCDC also recognises that children and vulnerable individuals may:

- Have limited ability to provide informed consent;
- Face heightened protection and confidentiality risks;
- Require additional safeguarding and privacy protections.

Accordingly, all child and vulnerable person information must be managed in accordance with:

- BCDC safeguarding obligations;
- Child protection principles;
- PSEAH obligations;
- Privacy and confidentiality requirements;
- Survivor-centred and do-no-harm approaches.

13. Photo, Video, and Media Consent

BCDC recognises the importance of protecting the dignity, safety, privacy, and informed consent of individuals whose photographs, videos, audio recordings, testimonials, stories, or media materials may be collected or used by the organisation.

The organisation will seek informed consent before:

- Taking photographs or video recordings;
- Recording audio materials;
- Publishing stories or testimonials;
- Using personal images or media content;
- Sharing materials through websites, reports, social media, fundraising, advocacy, or communication platforms.

Consent processes should:

- Be voluntary and informed;
- Be explained clearly and respectfully;
- Be appropriate to the person's language and understanding;
- Consider safeguarding and vulnerability risks;
- Allow individuals to decline participation where appropriate.

Where children or vulnerable individuals are involved, BCDC may seek consent from:

- Parents or guardians;
- Authorised caregivers;
- Responsible representatives;
- Appropriate safeguarding personnel where required.

BCDC will seek to avoid the use of images, stories, or media materials that:

- Exploit vulnerability or trauma;
- Compromise dignity or safety;
- Create safeguarding risks;
- Reveal sensitive protection-related information;
- Cause stigma, discrimination, or harm.

The organisation reserves the right to decline use of media materials where privacy, safeguarding, ethical, or reputational concerns are identified.

14. Use and Disclosure of Personal Information

BCDC may use personal information for purposes reasonably connected to:

- Service delivery and community support;
- Humanitarian and development activities;
- Safeguarding and protection processes;
- Volunteer or employment management;
- Program coordination and communication;
- Monitoring, evaluation, and reporting;
- Governance and compliance obligations;
- Financial and operational administration.

Personal information may be disclosed where:

- Consent has been obtained;
- Disclosure is necessary for operational purposes;
- Safeguarding or protection concerns require action;
- Legal or regulatory obligations apply;
- Emergency situations require disclosure to prevent harm.

BCDC will seek to ensure that disclosures of personal information are:

- Lawful and appropriate;
- Limited to relevant information only;
- Managed confidentially and securely;
- Consistent with safeguarding and privacy obligations.

The organisation will not sell, misuse, or improperly disclose personal information for unauthorised purposes.

15. Data Storage and Information Security

BCDC is committed to maintaining secure systems and procedures for storing, managing, protecting, and handling personal and confidential information.

Information may be stored:

- In physical records or filing systems;
- In password-protected electronic systems;
- In secure databases or cloud-based platforms;
- Through approved digital communication or record systems.

BCDC will take reasonable steps to:

- Prevent unauthorised access or disclosure;
- Protect information from misuse, loss, alteration, or destruction;
- Restrict access to authorised personnel only;
- Maintain secure passwords and access controls;
- Support secure handling of safeguarding and sensitive records.

Physical and digital records containing confidential or safeguarding-related information should be:

- Stored securely;
- Access-controlled;
- Managed responsibly;
- Retained in accordance with organisational and legal requirements.

The organisation also recognises that cyber risks, online threats, and data security failures may affect privacy and safeguarding outcomes. Accordingly, personnel are expected to follow organisational information security procedures and safe digital practices.

16. Internet, Website, and Digital Privacy

BCDC recognises the importance of maintaining responsible and secure digital privacy practices across websites, online platforms, social media, and electronic systems.

The organisation may collect limited digital or online information through:

- Website forms;
- Email communication;
- Online registrations;
- Surveys or digital engagement activities;
- Social media or communication platforms;
- Website analytics or technical usage information.

BCDC will seek to ensure that:

- Online information is collected lawfully and transparently;
- Website and digital systems are managed responsibly;
- Personal information shared online is protected where possible;
- Digital platforms are used safely and ethically;
- Safeguarding and privacy considerations are maintained in online activities.

The organisation may use reasonable website security measures and digital protection systems to:

- Reduce unauthorised access risks;
- Protect online information;
- Support secure communication and engagement;
- Monitor technical or cybersecurity risks.

Individuals using BCDC digital systems or platforms are expected to:

- Use systems responsibly;
- Respect privacy and confidentiality obligations;
- Avoid unauthorised sharing of sensitive information;
- Follow organisational digital safety procedures.

17. Email and Electronic Communications

BCDC recognises that email and electronic communication systems may contain personal, confidential, safeguarding-related, or sensitive organisational information.

Personnel using organisational communication systems are expected to:

- Communicate professionally and responsibly;
- Protect confidential information;
- Avoid unauthorised disclosure of personal information;
- Use secure communication practices where possible;
- Follow organisational privacy and safeguarding procedures.

Sensitive information transmitted electronically should:

- Be shared only where necessary;
- Be restricted to authorised recipients;
- Be handled using appropriate confidentiality precautions;
- Avoid unnecessary exposure or forwarding.

BCDC also recognises that electronic communications may create privacy, cybersecurity, safeguarding, or reputational risks if handled improperly. Accordingly, personnel are expected to exercise caution and responsible judgement when using:

- Email systems;
- Messaging platforms;
- Social media;
- Digital communication tools;
- Online file-sharing systems.

18. Access to and Correction of Personal Information

BCDC recognises that individuals may request access to personal information held by the organisation, subject to safeguarding, confidentiality, operational, or legal considerations.

Where appropriate and lawful, individuals may:

- Request access to their personal information;
- Request correction of inaccurate or incomplete information;
- Seek clarification regarding how information is used or managed.

Requests for access or correction should:

- Be made through appropriate organisational channels;
- Include sufficient information to identify the records requested;
- Be managed respectfully and confidentially.

BCDC may limit access to information where:

- Safeguarding concerns exist;
- Confidentiality obligations apply;
- Legal restrictions apply;
- Disclosure may place individuals at risk;
- Information relates to ongoing investigations or protection matters.

The organisation will seek to respond to reasonable requests in a timely and appropriate manner.

19. Confidentiality Obligations of Staff and Volunteers

All BCDC personnel are expected to maintain confidentiality regarding personal, organisational, safeguarding, operational, and sensitive information accessed through their involvement with the organisation.

Staff, volunteers, contractors, consultants, and partner representatives are expected to:

- Respect confidentiality obligations;
- Protect personal and sensitive information;
- Avoid unauthorised disclosure or misuse of information;
- Follow organisational privacy and safeguarding procedures;
- Handle records and communications responsibly.

Confidential information should not be:

- Shared unnecessarily;
- Discussed in inappropriate settings;
- Used for personal advantage;
- Disclosed outside authorised organisational processes.

BCDC recognises that breaches of confidentiality may:

- Place individuals at risk of harm;
- Damage trust and community relationships;
- Affect safeguarding and protection outcomes;
- Create legal, operational, or reputational risks.

Serious breaches of confidentiality may result in disciplinary, corrective, contractual, or safeguarding action.

20. Data Breaches and Incident Response

BCDC recognises that privacy or data breaches may create significant safeguarding, operational, legal, reputational, and protection risks.

A data breach may involve:

- Unauthorised access to information;
- Unauthorised disclosure or sharing;
- Loss of physical or electronic records;
- Cybersecurity incidents;
- Accidental release of confidential information;
- Misuse or destruction of personal data.

All suspected data breaches should be reported promptly through appropriate organisational reporting channels.

BCDC may take actions including:

- Initial assessment of the breach;
- Immediate containment or protection measures;
- Safeguarding risk assessment;
- Restriction of further access or disclosure;
- Internal investigation or review;
- Notification of affected individuals where appropriate;
- Referral to external authorities where legally required.

Where safeguarding or vulnerable individuals are involved, BCDC will prioritise:

- Protection from harm;
- Confidentiality and safety;
- Safeguarding response measures;
- Survivor-centred and do-no-harm approaches.

The organisation may also review incidents to:

- Strengthen privacy systems;
- Improve information security practices;
- Reduce future risks;
- Support organisational learning and accountability.

21. Third-Party Service Providers and Partners

BCDC may engage third-party service providers, contractors, consultants, technology platforms, partner organisations, or external support providers to support organisational operations, safeguarding activities, communications, administration, data management, or service delivery.

Where third parties may access personal or confidential information, BCDC will seek to ensure that:

- Appropriate confidentiality obligations are maintained;
- Personal information is handled responsibly and securely;
- Safeguarding and privacy expectations are respected;
- Access to information is limited to legitimate operational purposes;
- Reasonable information protection measures are implemented.

Third-party providers and partners are expected to:

- Respect privacy and confidentiality obligations;
- Protect personal and sensitive information from unauthorised access or disclosure;
- Follow applicable safeguarding and data protection expectations;
- Use information only for approved and lawful purposes.

BCDC will seek to avoid sharing unnecessary personal information and may take reasonable steps to assess privacy, safeguarding, and security risks associated with external providers or operational partnerships.

22. Cross-Border Information Sharing

BCDC recognises that some organisational activities, humanitarian operations, partnerships, referrals, or support processes may involve communication or information sharing across different countries or operational contexts.

Where cross-border information sharing is necessary, BCDC will seek to:

- Protect confidentiality and privacy obligations;
- Minimise unnecessary disclosure of personal information;
- Consider safeguarding and protection risks;
- Use secure communication or information-sharing methods where possible;
- Ensure information sharing is lawful, appropriate, and operationally necessary.

Particular care should be taken when handling:

- Refugee or asylum-related information;
- Safeguarding and PSEAH records;
- Information involving vulnerable individuals;
- Sensitive community or protection-related information.

BCDC recognises that some cross-border operational contexts may involve increased:

- Security risks;
- Surveillance risks;
- Privacy vulnerabilities;
- Safeguarding concerns;
- Risks to refugees or displaced persons.

Accordingly, personnel should exercise caution and responsible judgement when sharing information across borders or international operational environments.

23. Record Retention and Secure Disposal

BCDC is committed to maintaining appropriate record retention and secure disposal practices for personal, safeguarding, operational, and confidential information.

Records may be retained for purposes including:

- Operational and program management;
- Safeguarding and protection obligations;
- Legal or compliance requirements;
- Financial accountability;
- Monitoring, evaluation, and reporting;
- Organisational learning and governance.

The organisation will seek to ensure that:

- Records are retained only for appropriate and necessary periods;
- Sensitive information remains protected during retention;
- Access to records is restricted to authorised personnel;
- Disposal processes prevent unauthorised access or disclosure.

Secure disposal methods may include:

- Secure shredding of physical documents;
- Permanent deletion of electronic files;
- Removal of access permissions;
- Secure destruction of storage materials where appropriate.

Safeguarding, child protection, legal, or investigation-related records may require additional retention or protection measures in accordance with organisational obligations and applicable laws.

24. Complaints and Privacy Concerns

BCDC recognises that individuals may have concerns, questions, or complaints regarding:

- Privacy practices;
- Confidentiality management;
- Information handling;
- Consent processes;
- Data protection;
- Use or disclosure of personal information.

Individuals are encouraged to raise concerns through appropriate organisational channels.

Privacy-related concerns may include:

- Unauthorised disclosure of information;
- Incorrect or outdated records;
- Concerns regarding consent;
- Data security or confidentiality issues;
- Inappropriate use of photographs or media materials;
- Concerns regarding safeguarding-related information handling.

BCDC will seek to:

- Receive concerns respectfully and confidentially;
- Assess concerns fairly and appropriately;
- Take reasonable corrective action where necessary;
- Strengthen organisational privacy and safeguarding systems where lessons are identified.

Where appropriate, concerns may also be managed in conjunction with:

- Complaint handling procedures;
- Safeguarding procedures;
- Incident reporting mechanisms;
- Risk management processes.

25. Responsibilities

All individuals associated with BCDC share responsibility for protecting personal information, maintaining confidentiality, and supporting ethical information management practices.

Board Responsibilities

The Board is responsible for supporting governance oversight, accountability, safeguarding obligations, and implementation of organisational privacy and confidentiality expectations.

Executive Responsibilities

Executive leadership is responsible for:

- Supporting implementation of this policy;
- Maintaining appropriate privacy and information protection systems;
- Responding to significant privacy concerns or data breaches;
- Supporting safeguarding-informed information management practices.

Staff and Volunteer Responsibilities

Staff, volunteers, contractors, consultants, and partner representatives are expected to:

- Respect confidentiality obligations;
- Protect personal and sensitive information;
- Follow organisational privacy and safeguarding procedures;
- Report suspected privacy breaches or information security concerns;
- Handle information responsibly and professionally.

Safeguarding Responsibilities

Personnel involved in safeguarding activities are expected to:

- Protect safeguarding-related information carefully;
- Maintain survivor-centred and confidentiality-focused approaches;
- Restrict access to safeguarding records appropriately;
- Follow safeguarding reporting and protection obligations.

26. Monitoring and Review

BCDC recognises that effective privacy and information protection systems require ongoing monitoring, review, and continuous improvement.

The organisation may monitor:

- Compliance with privacy and confidentiality obligations;
- Information management practices;
- Data protection and storage systems;
- Safeguarding-related information handling;
- Consent and media management processes;
- Cybersecurity and digital privacy risks;
- Privacy incidents or breach trends.

Monitoring activities may include:

- Governance reviews;
- Internal audits or operational reviews;
- Safeguarding monitoring;
- Staff and volunteer feedback;
- Incident and breach analysis;
- Information security assessments.

Findings from monitoring and review activities may support:

- Strengthening privacy systems;
- Improving safeguarding protections;
- Enhancing staff awareness and training;
- Improving digital security practices;
- Reducing organisational risks;
- Supporting continuous improvement.

27. Related Policies and Procedures

This policy should be read together with:

- Child Safeguarding Policy;
- PSEAH Policy;
- Risk Management Policy;
- Complaint Handling Policy;
- Whistleblowing Policy;
- Human Resources Management Policy;
- Volunteer Manual;
- Code of Conduct;
- Financial Wrongdoing Policy;
- Incident Reporting Procedures;
- Cybersecurity or Information Security procedures where applicable;
- Media and Communication procedures;
- PMEL Policy;
- Due Diligence and Partnership procedures.

These policies collectively support:

- Ethical and lawful information management;
- Safeguarding and protection obligations;
- Confidentiality and privacy protection;
- Responsible organisational governance;
- Prevention of harm and exploitation.

28. Review and Update Process

This policy should be reviewed periodically to ensure that it remains:

- Effective and operationally appropriate;
- Safeguarding-informed;
- Consistent with legal and regulatory obligations;
- Aligned with ACFID requirements and sector good practice;
- Responsive to emerging privacy and digital security risks.

The policy may be reviewed:

- Annually;
- Following significant privacy incidents or data breaches;
- Following safeguarding or confidentiality concerns;
- Following operational or technological changes;
- Following legal or regulatory updates;
- Following governance or compliance reviews.

The review process may consider:

- Organisational learning and feedback;
- Changes in privacy or cybersecurity risks;
- Safeguarding and confidentiality obligations;
- Monitoring and incident findings;
- Emerging sector good practice.

BCDC is committed to continuously strengthening:

- Privacy and confidentiality systems;
- Information security practices;
- Safeguarding-related information protection;
- Ethical and responsible data management;
- Organisational accountability and transparency.

29. Appendices

Appendix A – Privacy and Confidentiality Agreement Form
Appendix B – Photo, Video, and Media Consent Form
Appendix C – Personal Information Collection Notice
Appendix D – Data Breach Reporting Form

Appendix A – Privacy and Confidentiality Agreement Form

Burmese Community Development Collaboration (BCDC)

Privacy and Confidentiality Agreement Form

Purpose

This agreement outlines the responsibilities of individuals associated with BCDC regarding the protection, confidentiality, ethical handling, and appropriate use of personal, safeguarding-related, operational, and organisational information.

All personnel are expected to maintain confidentiality and comply with BCDC privacy, safeguarding, and information protection obligations.

Part A – Personnel Information

Item	Details
Full Name	
Position / Role	
Department / Program	
Organisation (if partner representative)	
Contact Number	
Email Address	
Date Commenced	

Part B – Privacy and Confidentiality Obligations

I understand and acknowledge that during my involvement with BCDC, I may have access to confidential, personal, safeguarding-related, operational, or sensitive information relating to:

- Refugees, displaced persons, and community members;
- Children and vulnerable individuals;
- Staff, volunteers, and partners;
- Safeguarding and PSEAH concerns;
- Organisational operations and governance;
- Financial or operational records;

- Personal case information and communications.

I understand that confidential information may include:

- Personal information;
- Safeguarding records;
- Refugee or client information;
- Health or wellbeing information;
- Photographs, videos, or media materials;
- Investigation or complaint records;
- Passwords, files, databases, or electronic records;
- Other information not publicly available.

Part C – Agreement and Responsibilities

I agree that I will:

- Respect privacy and confidentiality obligations at all times;
- Handle personal and sensitive information responsibly and securely;
- Use information only for authorised organisational purposes;
- Prevent unauthorised access, sharing, copying, or disclosure of information;
- Follow BCDC safeguarding, privacy, and information security procedures;
- Maintain confidentiality during and after my involvement with BCDC;
- Protect safeguarding and PSEAH-related information carefully;
- Use secure communication and storage practices where possible;
- Report suspected privacy breaches, data breaches, or confidentiality concerns promptly;
- Respect the dignity, safety, and rights of individuals whose information is managed by BCDC.

I understand that confidential information must not be:

- Shared outside authorised organisational processes;
- Discussed in inappropriate settings;
- Used for personal advantage or unauthorised purposes;
- Published or disclosed without appropriate approval or consent.

Part D – Digital and Information Security Responsibilities

I acknowledge my responsibility to:

- Protect passwords and login credentials;
- Use organisational systems responsibly;
- Avoid unsafe sharing of confidential information online;
- Follow secure email and electronic communication practices;
- Protect physical and electronic records from unauthorised access;
- Report suspected cybersecurity or information security concerns.

Part E – Safeguarding and Media Protection

I understand that additional confidentiality obligations apply to:

- Child protection information;
- PSEAH concerns;
- Safeguarding incidents or investigations;
- Refugee or protection-related information;
- Photographs, stories, or media materials involving vulnerable individuals.

I agree not to:

- Use photographs, videos, or stories without appropriate consent;
- Share safeguarding-related information inappropriately;
- Disclose sensitive information that may place individuals or communities at risk.

Part F – Breach of Confidentiality

I understand that failure to comply with this agreement may:

- Create safeguarding or privacy risks;
- Harm individuals or communities;
- Damage organisational trust and integrity;
- Result in disciplinary, contractual, safeguarding, or corrective action.

Part G – Declaration

I confirm that I have read, understood, and agreed to comply with the BCDC Privacy Policy, safeguarding obligations, and confidentiality requirements.

I understand my responsibilities regarding the ethical and secure handling of personal, confidential, safeguarding-related, and organisational information.

Name	Signature	Date

Internal Use Only

Item	Details
Agreement Received By	
Position	
Date Received	
Stored Securely	Yes / No

Confidentiality Notice

This document contains confidential organisational information and should be stored securely in accordance with BCDC privacy, safeguarding, and record-keeping procedures.

Appendix B – Photo, Video, and Media Consent Form

Burmese Community Development Collaboration (BCDC)

Photo, Video, and Media Consent Form

Purpose

BCDC may use photographs, videos, audio recordings, testimonials, stories, interviews, or other media materials for purposes including:

- Community engagement;
- Organisational communication;
- Safeguarding and awareness activities;
- Reporting and donor accountability;
- Advocacy and public education;
- Training and educational materials;
- Social media, website, and promotional activities.

This form is intended to ensure that media materials are collected and used respectfully, ethically, safely, and with informed consent.

Part A – Participant Information

Item	Details
Full Name	
Preferred Name (if applicable)	
Age	
Gender (Optional)	
Contact Number	
Email Address	
Community / Organisation	
Program / Activity Name	
Date	

Part B – Parent or Guardian Information (If Participant Is Under 18)

Item	Details
Parent / Guardian Name	
Relationship to Participant	
Contact Number	
Email Address	

Part C – Consent for Media Collection and Use

I understand that BCDC may collect or use:

- Photographs;
- Video recordings;
- Audio recordings;
- Testimonials or stories;
- Interview materials;
- Online or printed communication materials.

I understand that these materials may be used for:

- Organisational reports;
- Safeguarding or awareness campaigns;
- Community engagement;
- Website and social media platforms;
- Training or educational purposes;
- Advocacy or fundraising activities;
- Donor or stakeholder reporting.

I understand that:

- Participation is voluntary;
- I may decline participation where appropriate;
- BCDC will seek to use materials respectfully and ethically;
- BCDC will seek to protect dignity, safety, and confidentiality;

- Sensitive safeguarding or protection-related information will not be shared inappropriately.

Part D – Consent Options

Please tick the applicable boxes.

Consent Item	Yes	No
I consent to photographs being taken		
I consent to video recording		
I consent to audio recording		
I consent to use of my story or testimonial		
I consent to use of media materials in printed reports		
I consent to use on BCDC website or social media		
I consent to use for training or educational purposes		
I consent to future organisational communication use		

Part E – Safeguarding and Confidentiality Considerations

Please indicate if there are any privacy, safeguarding, protection, or confidentiality considerations that BCDC should be aware of.

Examples may include:

- Refugee or protection-related concerns;
- Child safeguarding considerations;
- Cultural or family privacy concerns;
- Safety or security risks;
- Restrictions regarding online publication.

Part F – Special Restrictions or Conditions

Please specify any restrictions regarding:

- Social media use;
- Public identification;
- Name publication;
- Location information;
- Use of children's images;
- Online sharing or distribution.

Part G – Withdrawal of Consent

I understand that I may request withdrawal of consent in some circumstances by contacting BCDC, although materials already published or distributed may not always be fully removable.

BCDC will seek to manage withdrawal requests respectfully and reasonably where operationally possible.

Part H – Declaration and Signature

I confirm that:

- I have read and understood this consent form;
- I have had the opportunity to ask questions;
- I voluntarily provide consent as indicated above;
- The information provided is accurate to the best of my knowledge.

Participant Name	**Signature**	**Date**

Parent or Guardian Consent (If Applicable)

I confirm that I am the parent or authorised guardian of the participant named above and provide consent on their behalf.

Parent / Guardian Name	Signature	Date

Part I – Internal Use Only

Item	Details
Media Activity / Program	
Consent Received By	
Position	
Date Received	
Additional Safeguarding Review Required	Yes / No
Restrictions Recorded	Yes / No

Important Notice

BCDC is committed to ethical, respectful, safeguarding-informed, and dignity-focused use of photographs, stories, and media materials. The organisation reserves the right not to use materials where privacy, safeguarding, ethical, or protection concerns are identified.

Appendix C – Personal Information Collection Notice

Burmese Community Development Collaboration (BCDC)

Personal Information Collection Notice

Purpose

BCDC collects personal information to support its humanitarian, community development, safeguarding, operational, governance, and service delivery activities.

This notice explains:

- What information may be collected;
- Why information is collected;
- How information may be used;
- How information is protected;
- What rights individuals may have regarding their information.

BCDC is committed to handling personal information respectfully, securely, ethically, and in accordance with safeguarding and privacy obligations.

Information We May Collect

BCDC may collect personal or sensitive information including:

- Names and contact details;
- Emergency contact information;
- Demographic information;
- Refugee or migration-related information;
- Program participation records;
- Safeguarding or support-related information;
- Health or wellbeing information where appropriate;
- Photographs, videos, or media materials;
- Communication or engagement records.

The organisation will seek to collect only information that is:

- Relevant;
- Necessary;
- Lawful;
- Appropriate for operational or safeguarding purposes.

Why Information Is Collected

BCDC may collect information for purposes including:

- Service delivery and community support;
- Humanitarian and safeguarding activities;
- Program coordination and communication;
- Monitoring, evaluation, and reporting;
- Volunteer or employment management;
- Safety and emergency response;
- Governance and compliance obligations;
- Organisational communication and engagement.

Consent and Voluntary Participation

Where appropriate, BCDC will seek informed consent before collecting, using, storing, sharing, photographing, recording, or publishing personal information.

Participation in information collection or media activities is generally voluntary unless:

- Information is required for operational purposes;
- Safeguarding or protection obligations apply;
- Legal or compliance requirements require collection.

Individuals may ask questions or raise concerns regarding information collection processes at any time.

Confidentiality and Information Protection

BCDC is committed to protecting personal and sensitive information from unauthorised access, misuse, disclosure, or loss.

The organisation will seek to:

- Store information securely;
- Restrict access to authorised personnel;
- Protect safeguarding and confidential information carefully;
- Use information responsibly and ethically;
- Maintain confidentiality obligations.

Particular care will be taken regarding:

- Refugee and protection-related information;
- Safeguarding and PSEAH records;

- Information involving children or vulnerable individuals;
- Sensitive personal or community information.

Use and Disclosure of Information

Personal information may be used or shared:

- For legitimate organisational purposes;
- To support safeguarding or protection obligations;
- Where consent has been provided;
- Where disclosure is legally required;
- To prevent serious harm or risk.

BCDC will seek to avoid unnecessary disclosure of personal information and will handle information confidentially and responsibly.

Access and Correction Requests

Individuals may request:

- Access to their personal information;
- Correction of inaccurate or incomplete information;
- Clarification regarding how information is managed.

Requests may be limited where safeguarding, confidentiality, legal, or operational concerns apply.

Contact and Privacy Concerns

Questions, concerns, or requests relating to privacy, confidentiality, or information management may be directed to BCDC through appropriate organisational contact channels.

BCDC will seek to manage privacy-related concerns respectfully, confidentially, and in accordance with organisational policies and procedures.

Acknowledgement

I acknowledge that I have read or been informed about this Personal Information Collection Notice and understand how BCDC may collect, use, manage, and protect personal information.

Name	**Signature**	**Date**

Appendix D – Data Breach Reporting Form

Burmese Community Development Collaboration (BCDC)

Confidential Data Breach Reporting Form

Purpose

This form is used to report actual, suspected, or potential privacy breaches, confidentiality breaches, cybersecurity incidents, unauthorised disclosures, or information security concerns involving BCDC personal, safeguarding, operational, or confidential information.

All data breach concerns should be reported promptly to support:

- Protection of affected individuals;
- Safeguarding obligations;
- Risk reduction;
- Confidentiality and privacy protection;
- Organisational accountability and incident response.

Part A – Reporter Information

Item	Details
Full Name	
Position / Role	
Department / Program	
Contact Number	
Email Address	
Date of Report	

Part B – Incident Information

Item	Details
Date of Incident	
Time of Incident	
Location / System Involved	
Type of Incident	
How Was the Incident Identified?	

Part C – Type of Data Breach

Please tick all relevant categories.

Breach Type	Tick
Unauthorised access to information	
Unauthorised disclosure or sharing	
Lost or stolen documents	
Lost or stolen device	
Email sent to incorrect recipient	
Cybersecurity or hacking incident	
Safeguarding information exposure	
Child protection information breach	
Refugee or client confidentiality breach	
Media or photograph misuse	
Password or account compromise	
Improper disposal of records	
Other privacy or confidentiality concern	

Part D – Description of the Incident

Please describe:

- What happened;
- What information was involved;
- How the incident occurred;
- Who may have been affected;
- Any immediate safeguarding or confidentiality concerns.

Part E – Information Potentially Affected

Please indicate the type of information involved.

Information Type	Tick
Personal information	
Contact information	
Refugee or protection-related information	
Safeguarding or PSEAH information	
Child protection information	
Health or wellbeing information	
Financial information	
Organisational operational information	
Photographs, videos, or media materials	
Passwords or login credentials	
Other sensitive information	

Part F – Immediate Risk Assessment

Question	Yes	No	Comments
Does the incident involve safeguarding risks?			
Are children or vulnerable individuals affected?			
Is confidential information publicly exposed?			
Is immediate action required?			
Does the incident involve cybersecurity concerns?			
Is external reporting required?			

Part G – Immediate Actions Taken

Please describe any immediate actions already taken to:

- Contain the breach;
- Protect affected individuals;
- Restrict access;
- Recover information or devices;
- Reduce further risks.

Part H – Additional Support or Escalation Required

Required Action	Tick
Safeguarding review required	
IT or cybersecurity support required	
Executive escalation required	
Legal or compliance review required	
External reporting required	
Risk management review required	
Communication support required	
Other action required	

Part I – Declaration

I confirm that the information provided in this report is accurate to the best of my knowledge and belief.

Name	Signature	Date

Part J – Internal Use Only

Item	Details
Report Received By	
Date Received	
Incident Reference Number	
Initial Risk Rating	Low / Moderate / High / Critical
Immediate Protective Measures Implemented	
Safeguarding Escalation Required	Yes / No
Investigation or Review Required	Yes / No
Outcome / Follow-Up Actions	

Confidentiality Notice

This document contains confidential and potentially sensitive information and must be handled securely in accordance with BCDC privacy, safeguarding, and information security obligations.