



Children Relief Service (CRS)

Dzaleka Dowa, P.O Box 16 Dowa, Malawi

DATA PROTECTION & CONFIDENTIALITY POLICY

Organization: Children Relief Service (CRS)

Location: Dzaleka-Lilambwe, Dowa District, Malawi

Email: info@childrenreliefmalawi.org

Phone/WhatsApp: +265 993 73 45 42

Website: childrenreliefmalawi.org

1. Introduction

At Children Relief Service (CRS), we work closely with children, young people, women, families, refugees, host communities, volunteers, schools, community leaders, partners, and other people who trust us with their information.

In our daily work in Dzaleka and surrounding communities, we may receive information about a person's family, education, health, protection concerns, financial situation, disability, personal circumstances, or experiences of abuse and violence. Some of this information is highly private and may affect a person's safety and dignity if it is disclosed to the wrong person.

We therefore understand that protecting information is not only an administrative responsibility. It is part of protecting people.

CRS is committed to handling personal information responsibly, respectfully, and securely. We collect and use information only when there is a legitimate reason to do so, protect it from unnecessary access or disclosure, and treat confidentiality as an important part of our responsibility to the people we serve.

This policy supports CRS's commitment to child protection, safeguarding, dignity, inclusion, accountability, and responsible programming.

2. Purpose of the Policy

The purpose of this policy is to ensure that personal information entrusted to CRS is:

- Collected responsibly and for legitimate purposes
- Used only for appropriate and clearly understood purposes
- Kept accurate and relevant
- Protected against unauthorized access, loss, misuse, alteration, or disclosure

- Shared only when there is a legitimate reason and appropriate authorization
- Kept confidential, particularly where disclosure could place someone at risk
- Stored securely for as long as necessary
- Safely destroyed or deleted when it is no longer needed

This policy also helps our staff, volunteers, representatives, and partners understand their responsibilities when handling personal information.

3. Scope

This policy applies to everyone working with or representing CRS, including:

- Board members
- Founder & Executive Director
- Staff members
- Programme officers
- Volunteers
- Interns and trainees
- Consultants and technical advisors
- Community workers and representatives
- Anyone who handles personal information on behalf of CRS

It applies to information collected or handled through:

- Programme activities
- Registration and assessment forms
- Child protection and safeguarding activities
- Education programmes
- Vocational and skills training
- Food security and livelihood programmes
- GBV prevention and response activities
- Community outreach
- Surveys and assessments
- Monitoring and evaluation
- Photography and video activities
- Emails, WhatsApp, social media, and other digital communication
- Paper records and files
- Computers, phones, storage devices, and other electronic systems

4. What We Mean by Personal Information

Personal information is information that identifies a person or can reasonably be used to identify them.

This may include:

- Name

- Photograph or video
- Telephone number
- Email address
- Home or community information
- Date of birth or age
- Family information
- Education information
- Identification information
- Disability-related information
- Health-related information
- Financial or livelihood information
- Case or programme information
- Information about protection concerns
- Information concerning abuse, exploitation, or violence
- Information relating to survivors of gender-based violence
- Any other information that could identify or expose a person

Some information requires additional care because disclosure could cause harm, discrimination, embarrassment, retaliation, stigma, or other protection risks.

5. Our Commitment to Confidentiality

At CRS, confidentiality means that information entrusted to us is treated with respect and is not casually discussed, copied, photographed, shared, or disclosed.

A staff member or volunteer should never discuss a person's private circumstances simply because they know the information.

For example, information about a child's protection concern should not be discussed with friends, other community members, unrelated programme participants, or on social media.

Similarly, information about a survivor of gender-based violence must be handled with particular care. A person's story belongs to that person. Their experience must never become a subject of gossip, entertainment, publicity, or unnecessary discussion.

Confidentiality applies inside and outside the CRS office, including during community activities, meetings, home visits, training sessions, WhatsApp conversations, telephone calls, and informal discussions.

6. Collecting Information Responsibly

CRS will make reasonable efforts to collect only information that is necessary for the legitimate purpose for which it is being collected.

Before collecting information, staff should consider:

- Why do we need this information?

- Is it necessary for our programme or responsibility?
- Do we need all of the information being requested?
- How will the information be used?
- Who will have access to it?
- How will it be protected?
- How long will we need to keep it?

We should avoid collecting information simply because it may be useful someday.

Where appropriate, people should be given clear and understandable information about why their information is being collected and how it will be used.

7. Children and Young People

Children require special protection when their personal information is collected or used.

CRS staff and volunteers must take particular care when handling information about children, especially information relating to:

- Protection concerns
- Abuse or neglect
- Family circumstances
- Health
- Disability
- Education
- Case management
- Photographs and videos
- Personal identification
- Any other information that could place a child at risk

Information about a child must only be accessed or shared by people who have a legitimate reason to receive it.

Children must never be identified publicly in a way that could expose them to harm, stigma, exploitation, retaliation, or unnecessary attention.

Where consent or permission is required for photographs, stories, publications, or other uses of a child's information, CRS will follow appropriate safeguarding and consent procedures.

8. Survivors and Sensitive Protection Information

CRS recognizes that people affected by gender-based violence, abuse, exploitation, trafficking, or other protection concerns may face serious risks if their information is disclosed.

Information concerning survivors must therefore be handled with particular sensitivity.

Staff and volunteers must:

- Respect the survivor's dignity and privacy
- Avoid unnecessary questions
- Avoid sharing identifying information without a legitimate reason
- Keep case information secure
- Avoid discussing cases in public places
- Use appropriate referral and reporting channels
- Share information only when necessary and authorized
- Follow survivor-centered and safeguarding principles

No CRS staff member or volunteer should share a survivor's name, photograph, location, story, telephone number, or other identifying information simply for publicity or personal interest.

9. Photographs, Videos and Stories

Photographs, videos, testimonies, and personal stories can help CRS explain its work and show the impact of programmes.

However, people are more important than publicity.

CRS will therefore take reasonable steps to ensure that photographs, videos, and stories are collected and used respectfully and responsibly.

Staff and volunteers should not take or publish photographs of children, survivors, or vulnerable individuals simply because they are present at a CRS activity.

Before using photographs, videos, quotations, or personal stories publicly, CRS will consider:

- Whether the person understands how the material will be used
- Whether appropriate consent or permission has been obtained
- Whether publication could expose the person to harm
- Whether the person's dignity is protected
- Whether identifying information is necessary
- Whether the image or story could create stigma or embarrassment

CRS will never intentionally use a person's vulnerability as a way of attracting attention, sympathy, or funding.

10. Using WhatsApp, Email and Social Media

Digital communication is an important part of how CRS works with communities and partners. However, digital communication can also create privacy risks.

Staff and volunteers must therefore exercise care when using:

- WhatsApp
- Email
- Facebook
- X
- LinkedIn
- Other social media platforms
- Cloud storage
- Mobile phones
- Computers and other digital devices

Personal information should not be posted in public groups or social media platforms unless there is a legitimate and authorized reason to do so.

Sensitive information should not be forwarded to people who do not need it.

Staff should check recipients carefully before sending emails, documents, photographs, or other information.

Where possible, sensitive documents should be protected using appropriate security measures.

11. Access to Information

Not everyone working with CRS needs access to every piece of information.

CRS will follow a need-to-know approach.

This means that access to personal information should be limited to people who need the information to perform their legitimate responsibilities.

For example, a staff member working on an education activity does not automatically need access to confidential GBV case information.

A volunteer helping with a community event should not automatically have access to confidential child protection records.

Access should be based on responsibility, necessity, and authorization.

12. Storage of Information

CRS may maintain both paper and electronic records.

Paper records should be kept in secure locations where unauthorized people cannot easily access them.

Electronic information should be protected through appropriate measures such as:

- Strong passwords
- Restricted access
- Secure devices
- Appropriate user permissions
- Safe storage
- Regular backups where appropriate
- Responsible use of cloud services
- Protection against unauthorized sharing

Staff should not leave confidential documents openly visible on desks, community spaces, vehicles, or other locations where unauthorized people can access them.

Personal information stored on personal phones or computers for CRS work must also be handled responsibly.

13. Sharing Personal Information

CRS will not share personal information simply because someone asks for it.

Before information is shared, staff should consider:

- Is there a legitimate reason for sharing it?
- Is the person receiving it authorized to receive it?
- Is the information necessary?
- Could sharing it put someone at risk?
- Has appropriate consent or another lawful basis been established where required?
- Can less information be shared while still achieving the legitimate purpose?

Where information must be shared for safeguarding, referral, programme delivery, legal, or other legitimate purposes, CRS will seek to share only what is reasonably necessary.

14. Working With Partners

CRS works with schools, community structures, organizations, donors, service providers, government institutions, and other partners.

Where partners receive personal information from CRS or process information on behalf of CRS, appropriate safeguards should be considered.

CRS will seek to ensure that information shared with partners is:

- Relevant to the purpose
- Necessary
- Handled confidentially
- Shared through appropriate channels
- Protected from unauthorized use or disclosure

Partners should not use CRS information for purposes that have not been authorized.

15. Accuracy of Information

CRS recognizes that inaccurate information can affect people's access to services, opportunities, and protection.

We will therefore make reasonable efforts to keep personal information accurate and up to date.

Where a person identifies an important error in information held about them, CRS will consider the request and correct information where appropriate.

Staff should also avoid recording assumptions, rumours, or unverified allegations as established facts.

16. Retention and Disposal

CRS will not keep personal information indefinitely without a legitimate reason.

Information should be retained only for as long as it is reasonably required for the purpose for which it was collected, organizational accountability, legal requirements, safeguarding, programme requirements, or other legitimate purposes.

When information is no longer required, it should be securely destroyed, deleted, or otherwise disposed of in a way that prevents unauthorized recovery or access.

Paper records containing confidential information should not simply be thrown into ordinary rubbish where they could be read by others.

17. Data Breaches and Loss of Information

A data breach may occur when personal information is:

- Lost
- Stolen
- Accidentally sent to the wrong person
- Accessed without authorization
- Published accidentally
- Shared without authorization
- Altered or destroyed without permission
- Exposed through a compromised device or account

Staff and volunteers must report suspected or actual breaches to CRS leadership as soon as possible.

People should not hide mistakes because they are afraid of being blamed.

Reporting a problem quickly gives CRS a better opportunity to protect affected people, limit further disclosure, and take appropriate corrective action.

18. Responsibilities of Staff and Volunteers

Everyone working with CRS has a responsibility to protect information.

Staff and volunteers must:

- Treat personal information with respect
- Keep confidential information private
- Use information only for legitimate CRS responsibilities
- Protect documents and devices
- Follow access restrictions
- Avoid unnecessary copying or sharing
- Report suspected breaches
- Follow safeguarding procedures
- Ask for guidance when unsure about handling information

Confidentiality responsibilities continue even after a person stops working or volunteering with CRS.

19. Responsibilities of CRS Leadership

CRS leadership is responsible for promoting a culture in which privacy and confidentiality are taken seriously.

Leadership will work to:

- Provide appropriate guidance to staff and volunteers
- Promote responsible information handling
- Review data protection risks
- Establish appropriate access controls
- Respond to reported breaches
- Strengthen staff awareness and training
- Review this policy when necessary
- Promote compliance with applicable legal and organizational requirements

Where CRS grows its systems, programmes, partnerships, or digital activities, data protection should be considered as part of planning rather than treated as an issue only after a problem occurs.

20. Respect, Dignity and Do No Harm

For CRS, data protection is ultimately about people.

A database, registration form, case file, photograph, report, or spreadsheet may appear to be just information. Behind that information is a real person with a life, family, hopes, challenges, and rights.

A child whose name appears on a programme list is a child whose safety matters.

A woman whose information appears in a protection record is a person whose dignity matters.

A family that shares information with CRS because they need assistance is placing trust in our organization.

We must therefore ask not only, **"Can we collect or share this information?"** but also, **"Could this cause harm to the person?"**

CRS will seek to make decisions about personal information in a way that protects dignity, reduces risk, and respects the people we serve.

21. Reporting Concerns

Anyone who believes that personal information has been misused, lost, improperly disclosed, or accessed without authorization should report the concern to CRS leadership.

Concerns may be reported directly to:

Children Relief Service (CRS)

Dzaleka-Lilambwe, Dowa District, Malawi

Email: info@childrenreliefmalawi.org

Phone/WhatsApp: +265 993 73 45 42

Where the concern involves safeguarding, child protection, GBV, exploitation, abuse, or another protection issue, it should also be handled through the appropriate CRS safeguarding and referral procedures.

22. Non-Compliance

Failure to respect confidentiality and data protection requirements may place individuals at risk and may damage the trust that communities place in CRS.

Depending on the seriousness of the situation, inappropriate access, use, disclosure, or handling of personal information may result in corrective action or disciplinary measures in accordance with CRS procedures and applicable requirements.

Where a matter may involve unlawful conduct, CRS may take additional steps as appropriate.

23. Policy Review

CRS will review this policy periodically and whenever significant changes occur in its programmes, information systems, partnerships, legal requirements, or organizational structure.

The policy will be updated when necessary to ensure that it remains practical, relevant, and responsive to the realities of the communities CRS serves.

24. Our Commitment

At Children Relief Service, we know that trust is built slowly and can be lost quickly.

People share information with us because they believe that CRS will listen, respect them, and use their information responsibly.

We are committed to protecting that trust.

Whether information is written on a paper form in Dzaleka, stored on a computer, shared through a programme report, discussed during a case referral, or captured in a photograph, we will seek to handle it with the care, dignity, and responsibility that every person deserves.

Protecting information is part of protecting people.

Children Relief Service (CRS)

Dzaleka-Lilambwe, Dowa District, Malawi

info@childrenreliefmalawi.org

+265 993 73 45 42

childrenreliefmalawi.org

Policy Status: Organizational Policy

Review: Periodic review or when significant changes occur

Applies To: Board Members, Staff, Volunteers, Consultants, Advisors, Interns, and Representatives of CRS