PRIVACY RESPONSIBILITIES FOR CCM

Protecting Dignity and Confidentiality in Every Interaction

Introduction

Protecting personal information is a key responsibility for all involved in community care ministries (CCM). This guide outlines the privacy responsibilities of Corps Officers, CCM Coordinators, and volunteers to ensure compliance with The Salvation Army's privacy policies and applicable legislation.

Privacy Roles and Responsibilities

Corps Officers (Privacy Officers at the Corps Level)

- Act as the designated **Privacy Officer** for CCM within the Corps.
- Ensure that all CCM privacy policies align with TSA's GV 01.009 Privacy Policy and applicable privacy laws.
- Oversee the collection, use, and storage of personal information in CCM activities.
- Ensure all CCM Coordinators and Volunteers receive appropriate privacy training.
- Investigate and report privacy incidents or breaches to the Territorial Privacy Officer.
- Maintain records in accordance with IT 04.001 Data Retention Policy.

CCM Coordinators

- Implement privacy protocols in CCM programs, ensuring volunteers follow them.
- Maintain confidentiality agreements for all volunteers handling personal information.
- Limit access to personal information based on the need-to-know principle.
- Securely store and dispose of personal information as per IT 04.002 Data Destruction Policy.
- Train volunteers on privacy best practices and report privacy incidents to the Corps Officer.
- Best practice: The CCM Coordinator should be provided with a Salvation Army email address for official CCM communications, ensuring secure and professional handling of personal information.

CCM Volunteers

- Handle personal information with care, only accessing what is necessary.
- Never share personal details about those receiving CCM support outside of approved channels.
- Use designated Corps/TSA communication methods (avoid personal email or devices for sensitive information).
- Follow data retention and disposal policies.
- Report any privacy concerns or breaches to the CCM Coordinator or Corps Officer immediately.

Handling Personal Information

Collecting Personal Information

- Only collect essential information needed for CCM activities (e.g., name, contact details, health-related needs with consent).
- Obtain informed consent before collecting or using personal information.
- Inform individuals about how their information will be used and stored.

Storing Personal Information

- Paper Records: Keep in locked cabinets in secured locations.
- Electronic Records: Store only on TSA-approved, password-protected systems.
- Mobile Devices: Avoid storing personal information; if necessary, ensure encryption and immediate deletion after use.

Sharing Personal Information

- Share personal information only with authorized mission partners and only as required.
- Use secure channels (e.g., encrypted email, secure portals) when sharing information electronically.
- Do not discuss private details about individuals in public or unsecure settings.

Disposing of Personal Information

- Shred paper documents containing personal data when no longer needed.
- Delete electronic files securely as per IT 04.002 Data Destruction Policy.
- Follow TSA's Data Retention Schedule for record-keeping guidelines.

Communication and Privacy

Emails and Messaging

- Use official TSA email accounts for CCM communication.
- Do not include personal details in email subject lines.
- Encrypt sensitive emails and limit recipients to those who need-to-know.

Phone and Voicemail

- Avoid discussing personal information in open areas.
- Delete voicemails with sensitive content once actioned.
- Do not store or save personal details in unsecured phone contacts.

Faxing and Printing

- Confirm fax recipients before sending personal information.
- Retrieve printed documents immediately from shared printers.
- Store incoming faxes securely and dispose of outdated information promptly.

Responding to Privacy Incidents

What is a Privacy Incident?

A privacy incident includes:

- Unauthorized access, loss, or improper disclosure of personal information.
- Misplaced or improperly stored physical or electronic records.
- Accidental transmission of personal details to the wrong recipient.

Steps to Take if a Privacy Incident Occurs

1. **Report Immediately** to the CCM Coordinator or Corps Officer.
2. **Contain the Incident** (e.g., retrieve misdirected emails, lock records away).
3. **Document the Incident** and complete a **Privacy Incident Report**.
4. **Implement Corrective Measures** (e.g., additional training, process improvements).
5. **Notify Affected Individuals** if required by privacy laws or TSA policy.

Privacy Training and Compliance

- Corps Officers must ensure all CCM members are aware of **TSA privacy policies**.
- Regular **privacy audits** should be conducted to ensure compliance.

Volunteers should seek clarification on privacy concerns from the CCM Coordinator.

Conclusion

Privacy protection is essential for maintaining trust in Community Care Ministries. Corps Officers, CCM Coordinators, and Volunteers must uphold confidentiality, follow security protocols, and report any privacy concerns to ensure compliance with The Salvation Army's privacy policies.

For further guidance, contact the Corps Officer or TSA's Territorial Privacy Officer.