**Information Sharing Guidelines**

**Purpose**

These guidelines establish protocols for sharing sensitive information about residents and shelter operations while maintaining security, confidentiality, and dignity of survivors of gender-based violence.

**Core Principles**

**1. Confidentiality**

* All personal information about residents must be treated with strict confidentiality
* Information should only be shared on a need-to-know basis
* Written consent must be obtained before sharing any resident's information with external parties
* Staff must sign confidentiality agreements before accessing resident information

**2. Security Measures**

* All physical documents containing resident information must be stored in locked cabinets
* Digital information must be password-protected and encrypted
* Access to resident files must be restricted to authorized personnel only
* Shelter locations must not be publicly disclosed

**3. Informed Consent Requirements**

* Obtain written consent from residents before collecting any personal information
* Clearly explain how their information will be used and stored
* Inform residents of their right to decline information sharing
* Document all instances of consent given or withdrawn

**4. Data Collection Standards**

* Collect only essential information necessary for service provision
* Use standardized forms for consistent data collection
* Record information accurately and objectively
* Update resident information regularly

**5. Information Sharing Protocols**

Internal Sharing

* Share resident information during staff handovers using secure channels
* Conduct case discussions in private settings
* Use resident ID numbers instead of names in general communications
* Document all internal information sharing in resident files

External Sharing

* Share information with external partners only when:
* Required by law
* Necessary for resident safety
* Requested by resident with written consent
* Use encrypted emails or secure platforms for digital sharing
* Redact identifying information when sharing aggregate data

 **6. Documentation Requirements**

* Maintain detailed incident reports
* Keep accurate records of all services provided
* Document all external referrals and coordination
* Record any breaches of confidentiality

**7. Staff Training**

* Provide regular training on information handling
* Review confidentiality protocols quarterly
* Train new staff before granting access to resident information
* Document all training sessions and attendance

**8. Working with Law Enforcement**

* Establish protocols for responding to police inquiries
* Require proper documentation for information requests
* Consult with resident before sharing information
* Document all law enforcement interactions

**9. Media Guidelines**

* Never share resident information with media
* Protect shelter location in all external communications
* Obtain written consent for success stories or testimonials
* Remove identifying details from public communications

**10. Information Breach Protocols**

* Immediately report any confidentiality breaches
* Document the incident and response
* Notify affected residents
* Review and update security measures

**Implementation**

* Roles and Responsibilities
* Shelter Director: Overall responsibility for guideline implementation
* Case Managers: Daily information handling and resident file maintenance
* Security Staff: Physical document security
* IT Support: Digital security measures

**Monitoring and Compliance**

* Conduct quarterly audits of information handling practices
* Review and update guidelines annually
* Report compliance issues to shelter management
* Maintain records of all audits and reviews

**Emergency Procedures**

* Establish clear protocols for information handling during emergencies
* Maintain backup systems for critical information
* Define emergency contact procedures
* Review emergency protocols regularly

**Contact Information**

[Insert relevant contact details for:

Shelter Management

Emergency Services

Legal Support

Technical Support]

**Review and Updates**

These guidelines should be reviewed annually and updated as needed to reflect changes in:

* Legal requirements
* Best practices
* Technology
* Security needs

Last Updated: [Insert Date]