

AFFINITY™

Pastoral Care Privacy & Confidentiality Policy Manual

Privacy, Confidentiality, Records, and Information-Handling Standards

Official Program Policy Document

Issued October 2026

Brooks Consulting & Training Solutions, LLC

Dr. Vanessa R. Brooks

Purpose

The purpose of this policy is to establish clear standards for protecting the privacy and confidentiality of individuals receiving care through the AFFINITY™ Pastoral Care Program.

Pastoral-care information should be handled with respect, discretion, and only for legitimate care-related purposes.

1. Privacy Standard

Individuals receiving pastoral care have a reasonable expectation that personal information shared during the care process will be treated as private.

Pastoral-care information should only be collected when it is relevant to the person's care, safety, eligibility, referral, or follow-up.

Churches should avoid collecting unnecessary personal information.

2. Confidentiality Standard

Information shared during pastoral care should not be disclosed to people who are not directly involved in the care process.

Pastoral-care information should not be used for:

- gossip
- public discussion
- sermons or illustrations without appropriate permission and de-identification
- unrelated leadership conversations
- ministry promotion
- disciplinary action unrelated to the pastoral-care matter
- personal or organizational advantage

3. Who May Access Pastoral-Care Information

Access should be limited to individuals who have an authorized role in the pastoral-care process.

This may include:

- designated pastoral-care leaders
- approved ministry staff
- authorized pastoral-care volunteers
- church leadership when directly necessary for care, safety, or required decision-making
- outside professionals or community partners when appropriate consent has been provided

Access should be based on need to know, not position or curiosity.

4. Consent to Share Information

Whenever possible, the person receiving care should be informed before their information is shared with another person, ministry, professional, or organization.

Consent should be obtained when information is shared for purposes such as:

- referral
- professional collaboration
- coordination of services
- connection with another church ministry
- resource assistance that requires information to be disclosed

Only the information reasonably necessary for the intended purpose should be shared.

5. Limits of Confidentiality

Confidentiality is not absolute.

Information may need to be disclosed when:

- there is an immediate threat to the safety of the person or another individual
- abuse, neglect, exploitation, or another matter triggers a legal reporting obligation
- disclosure is required by applicable law or court order
- emergency intervention is necessary
- the individual has provided appropriate consent
- disclosure is necessary to carry out an authorized pastoral-care function

When disclosure is necessary, only information relevant to the situation should be shared whenever possible.

6. Pastoral-Care Records

Each individual receiving ongoing pastoral care should have a separate case file when documentation is necessary.

Case files may include:

- completed Pastoral Care Intake and Assessment Forms
- eligibility documentation
- referral forms
- resource documentation
- C5 Counseling Integration Framework™ documentation when applicable
- follow-up or continuation-of-care documentation

Case files should be kept separate from general church membership records whenever possible.

7. Storage of Physical Records

Physical pastoral-care records should be stored in a secure location with limited access.

Examples include:

- locked filing cabinets
- locked offices
- secured records rooms

Case files should not be left unattended in public or shared ministry spaces.

8. Storage of Digital Records

If a church maintains digital pastoral-care records, those records should be stored using reasonable security protections.

This may include:

- password-protected systems
- restricted user access
- secure church-approved cloud storage
- device security
- access controls based on staff roles

Pastoral-care records should not be stored on unsecured personal devices or shared through unsecured channels when safer alternatives are available.

9. Communication About Pastoral Care

Pastoral-care information should be communicated carefully.

Staff and volunteers should avoid discussing cases:

- in hallways
- in public spaces
- in group text messages not authorized for care coordination
- on social media
- with family members, friends, or church members who are not involved in care

Electronic communication should contain only the information necessary for the purpose of the communication.

10. Use of Pastoral-Care Information for Training or Teaching

Pastoral-care situations should not be used for training, teaching, presentations, or public examples in ways that could reasonably identify the individual without appropriate permission.

Whenever possible, identifying details should be removed or altered.

11. Case File Access

Individuals should not be permitted unrestricted access to pastoral-care case files simply because they hold a leadership position within the church.

Access should be determined by:

- assigned pastoral-care responsibility
- legitimate care need
- safety considerations
- authorized decision-making responsibility
- applicable church policy

12. Record Retention and Disposal

Each licensed church should establish a reasonable process for retaining and disposing of pastoral-care records.

When records are no longer required, they should be destroyed securely.

Examples include:

- shredding physical records
- permanently deleting digital records
- securely disposing of storage devices when necessary

Churches should consider applicable legal, insurance, denominational, and organizational requirements when establishing retention periods.

13. Privacy Violations

Suspected or confirmed breaches of pastoral-care privacy or confidentiality should be reported to the person responsible for overseeing the church's pastoral-care program.

The church should determine:

- what information was involved
- who had access
- whether further disclosure should be stopped
- whether the affected individual should be informed
- whether corrective action or additional training is needed

AFFINITY™ Privacy Standard

Pastoral-care information should be:

Collected Carefully • Shared Purposefully • Accessed Only When Necessary • Stored Securely • Protected Consistently

Every person operating within the AFFINITY™ Pastoral Care Program is responsible for protecting the dignity, privacy, and trust of the people receiving care.