

PNW Conference Policy on Disclosure of Personal Information

Effective Date: October 14, 2026 | **Version:** 1.0

Applies To: All conference staff, including part-time, temporary, and volunteer personnel who answer phones, respond to email, or otherwise field inquiries on behalf of the PNW Conference

Policy Owner: PNW Office of Communications



1. Purpose

The Pacific Northwest Conference holds personal information about clergy, lay members, church staff, and volunteers in trust. This policy protects that information from being disclosed to people who intend to use it for harassment, fraud, solicitation, or other harm, while still allowing the conference to function as a connectional body where members can reasonably reach one another.

This policy governs how staff respond to requests for:

- Personal contact information (home address, personal phone number, personal email, birthdate, etc.)
- Health, employment or appointment details not already public
- Access credentials to the PNW Conference's online Journal, which contains the personal information described above

2. Guiding Principle

When in doubt, do not disclose. No staff member will be faulted for declining to share information when a requester's identity or purpose cannot be verified. It is always acceptable to say, "I'm not able to share that directly, but I'd be glad to pass your message along."

3. Definitions

Personal information: Any information that identifies an individual and is not already published in a public-facing directory or website, including home address, personal cell or home phone number, personal email, birthdate, spouse/family names, and similar details found in the Journal.

Known person: Someone the staff member can personally verify as who they claim to be, through direct personal acquaintance, a recognized conference email domain, a documented prior relationship (e.g., appears in conference records as clergy, staff, lay leader, or church officer), or successful callback verification (Section 5).

Unknown or unverified requester: Anyone whose identity or affiliation cannot be confirmed through the means above, including first-time callers, unfamiliar email addresses, and anyone who declines to identify themselves fully.

The Journal: The PNW Conference's official online Journal and any password-protected version of it that includes clergy and lay members' personal information.

4. Requests from Known Persons

Staff may share requested personal information and provide the Journal password when the requester is a known person as defined above. Good practice still applies:

- Share only the specific information requested and needed. There is no obligation to volunteer additional details.
- Do not share exported lists with anyone unless it is for work requested or approved by an official conference board, agency, or executive staff member. The recipient of any lists must also abide by the requirements of this policy.

- If a known person is asking on behalf of someone else (e.g., "my colleague needs the Journal password"), verify that the actual end user is also someone the conference can identify, or direct the requestor to have that person contact the conference directly.
- Update the Journal password on a regular schedule (see Section 8) so that shared credentials do not remain valid indefinitely for someone who no longer has a legitimate need.
- Direct all questions regarding current or past Conference staff, including personal information, employment status, pay, time off, and benefits, to Human Resources.

5. Requests from Unknown or Unverified Persons

Do not release personal information or the Journal password to anyone who cannot be verified as a known person. Instead:

1. **Ask who they are trying to reach and why.** A legitimate request almost always survives this question; a person with harmful intent often will not.
2. **Take down the requester's own information:** full name, organization or church (if any), a callback phone number or email, and the reason for wanting to connect.
3. **Offer to relay the message.** Tell the requester that the conference will pass their name, contact information, and reason for reaching out to the person they're trying to contact, who can then decide whether and how to respond.
4. **Do not confirm or deny** whether the person they're asking about is a conference member, current appointment holder, or otherwise affiliated, beyond what is already publicly available (for example, a church's publicly posted pastor listing). Confirming someone's existence in PNW Conference records can be sensitive information in itself.
5. **Follow up promptly** by forwarding the message to the person being sought, through their known conference or church email, not through contact information supplied by the requester. Be clear that you are passing along information, not validation of the requester's identity.

If a caller or emailer pushes back, becomes insistent, or tries to create urgency ("this is an emergency," "I just need it right now"), that is a reason for additional caution, not an exception to this process. Genuine emergencies can still be routed through the relay process quickly.

6. Categories Requiring Extra Caution

Some information warrants a second check even when the requester is known, because the consequences of misuse are higher:

- **Home addresses and personal cell numbers.** Confirm the requester has a genuine need before sharing, even with known recipients, and consider whether a work address or a conference-forwarded message would suffice instead.
- **Information about a person who has asked the conference not to share their information,** or who is in an active safety, harassment, or clergy complaint matter. Route these requests to the Director of Communications rather than responding directly.
- **Requests from media, attorneys, law enforcement, or process servers.** Do not provide personal information directly. Take down contact information, the topic, and any questions they may have, and forward these requests to the Executive Director of Connectional Ministries.
- **Requests involving minors.** Any personal information about a minor connected to a clergy or lay member's household should not be disclosed through this process under any circumstances; refer to the PNW Conference's Safe Sanctuaries policy and to staff leadership.
- **Information about a current or past Conference staff member,** including personal information, employment status, pay, time off, and benefits, should be forwarded to Human Resources.

7. The Online Journal and Its Password

Because the Journal aggregates personal information for many individuals at once, its password is treated as more sensitive than any single person's contact details.

- Provide the password only to known persons with a legitimate conference-related reason to access it (clergy, lay members, church staff, and officers of the conference and its churches).
- Do not post the password publicly, include it in mass emails to lists that may include unverified recipients, or leave it in materials that could be forwarded outside the conference.
- Keep a record of when and to whom the password is distributed outside of routine, expected channels, so the conference can trace exposure if it is later misused.

8. Records of Requests

For any request that goes through the unknown-requestor process (Section 5), keep a brief note of the date, the requestor's stated name and contact information, who they were trying to reach, and the outcome. This is not meant to be burdensome. A shared log or simple email trail is sufficient. It allows the Conference to spot patterns, such as the same person repeatedly seeking contact with someone who has not responded, or attempts to contact that also occur through other Conference offices.

9. When Something Feels Wrong

Staff should trust their instincts. If a request feels like an attempt to locate someone who may not want to be found, involves a pattern of persistent or evasive behavior, or otherwise raises concern, staff should:

- Decline to share any information beyond confirming they will pass along a message.
- Notify the Director of Communications promptly.
- Preserve any related emails, voicemails, or notes.

No staff member will face negative consequences for erring on the side of caution or escalating a request that turns out to be legitimate.

10. Individuals Requesting Their Own Information

A person asking what personal information the Conference holds about themselves should be directed to the District Service Center for identity verification and fulfillment, consistent with the Conference's recordkeeping practices.

11. Training and Acknowledgment

All staff who may field these requests will review this policy upon hire and will sign an acknowledgment that they understand and agree to follow it. Questions about how to apply this policy to a specific situation should go to the Director of Communications.

12. Related Policies and References

- *The Book of Discipline of The United Methodist Church*, provisions on confidentiality of clergy records and the conduct of Conference business
- PNW Conference Safe Sanctuaries policy
- GCFA data privacy and recordkeeping guidance

This policy addresses the disclosure of personal information by PNW Conference Office staff. It is separate from and does not override any legal obligations regarding subpoenas, mandatory reporting, or law enforcement requests, which should always be directed to the conference chancellor before any response is given.