



Diocese of Gallup Official Email Policy

Version 1.1

Overview

The objectives of this policy are to outline appropriate and inappropriate use of the Diocese of Gallup's email systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws. This policy applies to all email systems and services owned by the Diocese of Gallup, all email account users/holders at the Diocese of Gallup (both temporary and permanent), and all organization email records.

Information, including information entrusted to the Diocese of Gallup by its clients, donors and business partners must be protected by taking reasonable and appropriate steps to ensure information's confidentiality, integrity, and availability. All members of the diocese's workforce and all information systems used by the Diocese of Gallup are required to comply with the information security policies.

Emails sent from the Diocese of Gallup or entities affiliated with the Diocese of Gallup should not counter any teachings of the Catholic Church and should comply with normal standards of professional and personal courtesy and conduct.

Scope

This policy addresses email sent from a Diocese of Gallup email address or via diocesan equipment and applies to all employees, volunteers, vendors, and agents operating on behalf of the Diocese of Gallup.

Monitoring and Confidentiality

The email systems and services used at the Diocese of Gallup are owned by the Diocese and are therefore its property. This gives the Diocese of Gallup the right and responsibility to monitor any and all email traffic passing through its email system. While the organization does not actively read end-user email, IT employees may inadvertently read email messages during the normal course of managing the email system.

In addition, backup copies of email messages may exist, despite end-user deletion, in compliance with the Diocese of Gallup's records retention policy. The goals of these backup and archiving procedures are to ensure system reliability and prevent business data loss.

In addition, the Diocese of Gallup may access and disclose, for legitimate business and/or legal reasons, any email or communication sent or received through Diocesan communication systems. If the Diocese of Gallup discovers or has good reason to suspect activities that do not comply with applicable laws or this policy, email records may be retrieved and used to document the activity in accordance with due process.

Use extreme caution when communicating confidential or sensitive information via email. Keep in mind that all email messages sent outside of diocesan systems become the property of the receiver. A good rule is to not communicate anything that you wouldn't feel comfortable being made public. Demonstrate particular care when using the "Reply" command during email correspondence. Even when a message has been deleted, it may still exist on a backup system; it may be restored, downloaded, recorded, or printed; or it may have been forwarded to someone else without its creator's knowledge.

Acceptable accounts

All email accounts or emails sent with the intent of conducting work for the Diocese of Gallup or affiliated entities must use an appropriate email address.

Examples of acceptable accounts may include:

- A parish or employee with the "@dioceseofgallup.org" web address. I.e., johnsmith@dioceseofgallup.org or nameofparish@dioceseofgallup.org
- A parish or employee with a parish or entity-associated account. I.e., johnsmith@sacredheartparish.org or secretary@nameofparish.org

Examples of email accounts that will no longer be acceptable for diocesan, parish, or diocesan-affiliated business include:

- An employee's personal account through gmail, Hotmail, or other email service
- An account created independently and controlled by a single person – i.e. parishdre@gmail.com
- An account created independently for a parish through a non-diocesan or non-parish affiliated email system – i.e. nameofparish@gmail.com

If you are unsure of how to create an approved email account, or have concerns about transferring old emails, contacts and other information from a non-approved address into a new address, the Diocese of Gallup is able to create an account for you or help guide you through the process of creating an approved email account. **Contact info here**

Usage

Checking messages

Important official communications are often delivered via email. As a result, employees of the Diocese of Gallup with email accounts should check their email in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling business- and role-oriented tasks.

Email users are responsible for their own mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to remove himself or herself from the list and is responsible for doing so in the event that their current email address changes.

Forwarding and Auto-Forwarding of Email

Diocesan email should not be automatically forwarded. Sensitive information should not be forwarded via any means, unless that email is critical to business.

Retention

Employees should clean out their mailboxes periodically by filing the messages elsewhere using an appropriate archiving and organizing process or by deleting them. Certain message and attachments should be retained, either permanently or for a certain period of time. Please see the Diocese of Gallup email retention policy for guidance.

Backups and Recovery

The Diocese of Gallup does not actively maintain backups of email servers and deleted emails. Messages required to be kept for business reasons should be downloaded to another format and appropriately stored, and/or archived in an appropriate email folder separate from an account's inbox or deleted message folder.

Signatures

Process any correspondence or forms that require authenticating signatures or initials in paper form and not by e-mail, unless electronic signatures are specifically permitted. Attaching signed, scanned, documents should only be sent to trusted recipients.

Security

The following guidelines are good to keep in mind when sending and receiving emails, especially those of a sensitive nature.

- Do not assume a message will receive priority handling simply because you transmitted it electronically.

- Do not assume that information sent electronically is secure; there is no way of knowing who will see the e-mail at the recipient location or to whom it may be forwarded.
- Never open any e-mail or e-mail attachment from a source that you are not familiar with or were not expecting.
- Do not disclose User IDs and passwords to unauthorized parties or share with other employees, students, or volunteers. User accounts are intended to be used only by the assigned party.
- Change passwords to user accounts regularly.
- Avoid using the same password for user accounts with different providers.

Appropriate Use of Email

Use of the Diocese of Gallup's electronic mail systems and services must be used with respect and in accordance with the teaching of the Catholic Church and the goals of the diocese.

Examples of encouraged activities include:

- Communicating with fellow employees, donors, business partners, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

Prohibited Use of Email

Diocesan email use should comply with all applicable laws, diocesan policies, and teachings of the Catholic Church.

Examples of inappropriate activities include:

- Any message that can be construed to be harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, religious beliefs, or other personal characteristics or circumstances.
- Sexually-explicit messages, cartoons, or jokes
- Use of email for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses).
- Use of email to conduct, promote or otherwise support personal, for-profit business activities.
- Unsolicited mass emails, mailings, political campaigning, dissemination of chain letters, and use by non-employee members.

Employees who receive any emails with this content from any Diocese of Gallup employee or affiliated entity should report the matter to their supervisor immediately.

Personal Use

The Diocese of Gallup allows limited personal use of Diocesan email systems for independent learning and public service so long as it does not interfere with employee productivity, preempt any business activity, or consume more than a trivial amount of resources.

Diocesan email accounts should not be used for personal correspondence. The Diocese may provide accounts for staff and volunteers as needed. All diocesan business communications are property of the Diocese; intermixing personal correspondence is prohibited. Parish or organization-affiliated email accounts may be created if used strictly for business communication and all related security and privacy policies are observed.

Enforcement

Any employee or member who is found, after appropriate investigation, to have violated this policy may be subject to appropriate disciplinary action, including, but not limited to, one or more of the following:

- Temporary or permanent revocation of email access;
- Termination of employment; and/or
- Legal action according to applicable laws and contractual agreements.

Terms

Diocesan Communication Systems: Any email account, device, network or messaging system – including but not limited to social media accounts and phones – created or owned by the Diocese of Gallup.

Electronic Mail: Includes all electronic mail systems supported by the Diocese of Gallup or affiliated entities.

Email: The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Gmail, Microsoft Outlook, and Apple Mail.

Forwarded email: Email re-sent from an internal network to an outside point.

Chain email or letter: Email sent to successive people. Typically, the body of the note has the directive to send out multiple copies of the note and promises good luck or money if the directive is followed.

Insecure Internet Links: Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of the Diocese of Gallup.

Sensitive information: Information is considered sensitive if it contains personal details about a person or entity, or can be damaging to Diocese of Gallup, its parishioners, staff or public reputation or that of the Catholic Church in general.

Virus warning: Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

Unauthorized Disclosure: The intentional or unintentional revealing of restricted information to people, both inside and outside Diocese of Gallup, who do not have a need to know that information.

Spam: Electronic junk mail or junk newsgroup postings; more generally as any unsolicited e-mail; generally, e-mail advertising for some product sent to a mailing list or newsgroup.