Diocese of Pensacola-Tallahassee Email Use Policy

1.0 Purpose
To prevent tarnishing the public image of Diocese of Pensacola-Tallahassee when email is sent from the Diocese or any diocesan entities, appearance and content of those messages need to be professional and follow the guidelines of the teachings of the Catholic Church. The general public will tend to view that message as an official policy statement from the Diocese of Pensacola-Tallahassee. Keep this in mind when composing messages. We also try to control the transmission of viruses and other malware via email with this policy and prevent the unauthorized or inadvertent disclosure of sensitive company information.

2.0 Scope
This policy addresses email sent from a Diocese of Pensacola-Tallahassee email address or via diocesan equipment and applies to all employees, volunteers, vendors, and agents operating on behalf of Diocese of Pensacola-Tallahassee.

3.0 Policy
3.1 Prohibited Use. The Diocese of Pensacola-Tallahassee email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs or national origin. Employees who receive any emails with this content from any Diocese of Pensacola-Tallahassee employee should report the matter to their supervisor immediately. Diocesan email and email systems are not to be used to conduct, promote or otherwise support personal, for-profit business activities.

3.2 Personal Use.
Using a reasonable amount of Diocese of Pensacola-Tallahassee resources for personal emails is acceptable, but diocesan email accounts and addresses are not to be used for personal correspondence. Non-work related email shall be saved in a separate folder from work related email. Sending chain letters or non-professional emails from a Diocese of Pensacola-Tallahassee email account is prohibited as is any solicitation for personal endeavors. Any mass mailings, pertaining to virus or other malware warnings or messages regarding diocesan activities from Diocese of Pensacola-Tallahassee email accounts shall be approved by the appropriate diocesan director before sending. These restrictions also apply to the forwarding of mail received by a Diocese of Pensacola-Tallahassee employee.

3.3 Monitoring
Diocese of Pensacola-Tallahassee employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Diocese of Pensacola-Tallahassee may monitor messages without prior notice. Accessing personal email accounts using diocesan network connections is not excluded from this policy; all business rules still apply. Diocese of Pensacola-Tallahassee is not obliged to monitor email messages.

3.4 Non-business Email Accounts Used for Diocesan Business
The Diocese does not allow personal email accounts to be used for diocesan business. The Diocese provides accounts for all staff and volunteers as needed. All diocesan business communications are property of the Diocese; intermixing personal correspondence is prohibited. Non-diocesan sponsored email accounts may be created if used strictly for business communication and all related security and privacy policies are observed.

3.5 Auto-Forwarding of Email
Employees must exercise utmost caution when sending any email from inside the Diocese of Pensacola-Tallahassee to an outside network. Diocese of Pensacola-Tallahassee email will not be automatically forwarded. Sensitive information should not be forwarded via any means, unless that email is critical to business and is encrypted.

4.0 Usage

4.1 Checking messages

Employees should check mailboxes at least once a day (more frequently if possible) during normal working hours. Electronic mail should be treated and processed in the same manner as paper correspondence.

4.2 Retention

Normal business correspondence is to be kept no longer than six months in an active Inbox on a diocesan email server and may be deleted from email servers after that time. Employees should clean out their mailboxes periodically by filing the messages elsewhere using an "archiving" process or deleting them. It is Diocesan policy that attachments to email messages are to be downloaded and the original message deleted after reading. The USCCB has specific guidelines regarding the retention of documents which takes precedence over diocesan policy.

4.3 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 and may require encryption, depending on signature and content. Do not send anything via the e-mail system that is confidential or contains sensitive information. 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.

4.4 Mass Emailing – Spam

Sending more than 100 messages to multiple addresses with the exact same content, by today's Internet standards, is considered to be spam. This includes bulletins, newsletters, notices, etc. Information of this type should be posted on parish web sites or blogs, not sent via email. The consequence of being labeled as spam is messages from you will be rejected by the ISP of your intended recipients. The recovery from this process is not immediate; significant time, effort and expense can be required.

4.5 Recovering Deleted Email via Backup Media

Diocese of Pensacola-Tallahassee does not actively maintain backups of email servers. Messages required to be kept for business reasons are to be downloaded to another format and appropriately stored. No effort will be made to recover messages from email systems without legal obligation to do so.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Approved Electronic Mail	Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.
Email	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Gmail and Microsoft Outlook.
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 direction to send out multiple copies of the note and promises good luck or money if the direction 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 Diocese of Pensacola-Tallahassee.
Sensitive information	Information is considered sensitive if it can be damaging to Diocese of Pensacola-Tallahassee, 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 Pensacola-Tallahassee, 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.

7.0 Revision History

1 July 2012: Section 3.4: Addition: 3.4 Non-business Email Accounts Used for Diocesan Business. The Diocese does not allow personal email accounts to be used for diocesan business. The Diocese provides accounts for all staff and volunteers as needed. All diocesan business communications are property of the Diocese; intermixing personal correspondence is prohibited. Non-diocesan sponsored email accounts may be created if used strictly for business communication and all related security and privacy policies are observed.
18 July 2013: Section 1.0: Addition: . We also try to control the transmission of viruses and other malware via email with this policy and prevent the unauthorized or inadvertent disclosure of sensitive company information.
18 July 2013: Section 2.0: Change: This policy addresses ~~covers appropriate use of any~~ email sent from a Diocese of Pensacola-Tallahassee email address or via diocesan equipment and applies to all employees, volunteers, vendors, and agents operating on behalf of Diocese of Pensacola-Tallahassee.
18 July 2013: Section 3.5: addition: 3.5 Auto-Forwarding of Email
Employees must exercise utmost caution when sending any email from inside the Diocese of Pensacola-Tallahassee to an outside network. Unless approved by the I.T. Department, Diocese of Pensacola-Tallahassee email will not be automatically forwarded to an external destination. Sensitive information should not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with Diocesan Encryption Policy
March 19, 2014: Section 3.1: delete: gender, hair color, disabilities, age, sexual orientation,
May 22, 2015: Section 4.0: Change: renumbered and moved from 4.0 to 6.0, renumbered section 6.0 and 7.0 as 7.0 and 8.0
May 22, 2015: Section 5.0: Change: renumbered 5.0 to 4.0
May 22, 2015: Section 5.2: Addition: **in an active Inbox on a diocesan email server and may**
May 22, 2015: Section 5.2: Addition: **using "archiving" process**
May 22, 2015: Section 5.2: Delete: See the Diocesan *Email Retention Policy* for further details.
May 22, 2015: Section 5.2: Delete: It is also policy that messages between individuals or among a group of correspondents that is transmitted with "replies," are to be deleted as newer messages are received. Only the latest message with all previous comments and inputs should to be kept for the duration of the project or conversation.
May 22, 2015:Section 5.2: Addition: **The USCCB has specific guidelines regarding the retention of documents which takes precedence over diocesan policy.**
May 22, 2015: Section 7.0: Addition: **, its parishioners, staff or public reputation or that of the Catholic Church in general.**
May 22, 2015: Section 7.0: Delete: its customers' reputation or market standing.
May 22, 2015: Section 5.5: Addition: **new section from retired policy "Email Retention"**
Sep 27, 2017: Section 1.0: Addition**: appearance and content of those messages need to be professional and follow the guidelines of the teachings of the Catholic Church. The**
Sep 27,,2017: Section 6.0: Change: ~~**Eudora**~~ **Gmail**
Sep 27, 2017: Section 6.0: Change: ~~Email resent~~ **Email re-sent**
Sep 27, 2018: Section 1.0: change: ~~goes out~~ **is sent**
Sep 27, 2018: Section 3.5: Delete: in accordance with Diocesan Encryption Policy
Jul. 26, 2019: Section 3.2: Change: ~~joke emails~~ changed to non-professional emails
Jul. 26,2019: Section 3.5: Delete: Unless approved by the I.T. Department and to an external destination