

 ARCHDIOCESE OF SAINT PAUL & MINNEAPOLIS	Effective Date: 9/8/2026	Number: 201
	Subject: Acceptable Use and Responsibility Policy for Electronic Communications	
	Scope: ☒ Archdiocese ☐ Parishes ☐ Schools	
	Reference: Archdiocesan Employee Handbook	
Archbishop Signature: 		

Purpose

The purpose of this policy is to provide guidance regarding the use of technology to include computers, electronic devices, Artificial Intelligence (AI), and the screening of electronic devices.

Policy

All information used in the course and scope of activities on behalf of the [Archdiocese](#) is an asset of the [Archdiocese](#). The [Archdiocese](#) maintains a system of information security to protect proprietary data. Integral parts of this system are the policies, standards and procedures designed for [Users](#). All [Users](#) must adhere to these policies, standards and procedures. These policies, standards and procedures include maintaining data confidentiality, maintaining the confidentiality of data security controls and passwords, and immediately reporting any suspected or actual security violations. The [Archdiocese](#) prohibits the use or alteration of [Archdiocese](#) data or information technology without proper authorization. All [Users](#) have an obligation to protect the confidentiality and nondisclosure of proprietary, confidential and privileged data, as well as personally identifiable information.

I. SCOPE

- 1) This policy applies to:
 - a) All [Archdiocese](#) electronic systems, devices and materials located both on or off of [Archdiocese](#) property;
 - b) All [Users](#); and
 - c) All personal devices and materials, regardless of where they are located, that are used in the course and scope of [Archdiocese](#) activities.
- 2) The [Archdiocese](#) will maintain a record of electronic devices that are [Archdiocese](#) property in the possession of [Clergy](#), [Employees](#), or [Adult Volunteers](#).

II. OWNERSHIP, ENFORCEMENT AND RIGHT TO INSPECT

- 1) All [Archdiocese](#) systems, devices and materials, and all work performed on behalf of the the [Archdiocese](#) are property of the [Archdiocese](#). [Archdiocese](#) systems, devices, and materials are to be used primarily to conduct official [Archdiocese](#) business.
- 2) The [Archdiocese](#) reserves the right to monitor, access, retrieve, read, and disclose content created, sent, received, or stored on [Archdiocese](#) systems, devices, and materials (including connections made and sites visited) and to share such information with law enforcement or others, without prior notice.
- 3) When the [Archdiocese](#) has reasonable cause to believe that a [Cleric](#), [Archdiocese Employee](#) or volunteer has violated policies relating to electronic devices or their usage in a manner that involves sexual misconduct with a [Minor](#), the [Archdiocese](#) shall cooperate with law enforcement to preserve the electronic device for evidentiary value.
- 4) [Users](#) have no expectation of privacy in Archdiocesan systems, devices and materials. The [Archdiocese](#) may inspect, review, audit, intercept, or access all [Archdiocese](#) systems, devices and materials at any time, with or without notice.

III. GUIDELINES FOR ACCEPTABLE USE OF TECHNOLOGY

- 1) All [Users](#) should use care in creating email, text, video, still images, instant, or voice mail messages or in any postings on any social networking site. (See [Archdiocese](#) Employee Handbook 5-17). Even when a message has been deleted, it may still exist on a backup system; be restored, downloaded, recorded, or printed out; or have been forwarded to someone else without its creator's knowledge. The contents of email and text messages are the same as other written documentation and should not be considered private or confidential.
- 2) Mass emails or intranet/extranet/Internet postings to "All Employees," and the like must be approved by the appropriate department director and done in coordination with the [Archdiocese](#) Office of Communications before they are sent.
- 3) All [Archdiocese Employees](#) are required to use their [Archdiocese](#)-issued email account when sending any communication related to their job functions.
- 4) Use of personal electronic communications devices and materials while working should be kept to a minimum and should not interfere with work duties.
- 5) [Archdiocese](#) systems, devices, and materials are not private and security cannot be guaranteed. Passwords and user IDs are intended to enhance system security; not to provide [Users](#) with personal privacy. User IDs and passwords should not be disclosed to unauthorized parties. User accounts are intended to be used only by the assigned party.
- 6) Computer networks must be protected from unauthorized use. Both local physical access and remote access must be controlled.
- 7) Information systems hardware must be secured against unauthorized physical access.

- 8) [Minors](#) are prohibited from using [Archdiocese](#) devices or materials unless authorized and supervised by a [Cleric](#), [Employee](#) or [Adult Volunteer](#).
- 9) [Users](#) shall immediately report any viruses, tampering, or other system breaches to the IT (Information Technology) Department.
- 10) [Users](#) who post or distribute communications on social media or public websites must comply with the Archdiocese Employee Handbook “Use of Social Media” section (5-17).
- 11) Personal or unvetted AI services are prohibited for handling work-related data. Users must not input confidential, sensitive, or personally identifiable information (PII) into any AI system unless explicitly authorized by the manager of the User. Users are responsible for verifying AI-generated content. AI outputs must not be presented as factual without human review.

IV. PROHIBITED PRACTICES/UNACCEPTABLE USE

While using [Archdiocese](#) electronic systems, devices, or materials, or using personal devices and materials in the course and scope of [Archdiocese](#) duties and activities, [Users](#) may not:

- 1) Violate any federal, state or local laws or regulations.
- 2) Violate any Archdiocesan [Codes of Conduct](#).
- 3) Post or cause to be distributed any personally identifying information about another person without permission of that person, or the person’s parent or guardian if the person is under 18, unless doing so is required or concordant with the [User’s](#) job duties or assigned responsibilities. Personal identifying information includes images, names or screen names; telephone numbers; social security numbers, home or workplace addresses; and email addresses. Engage in pirating or unauthorized copying, acquisition, or distribution of copyrighted, trademarked, patented materials, music, video, or film or upload, download, view, or otherwise receive or transmit trade secrets, or other confidential, private, or proprietary information or other materials to which the [User](#) does not have access rights. Regarding copyrighted materials, certain exceptions are given for educational and liturgical purposes. It is the responsibility of the [User](#) to determine copyright status.
- 4) Post or send chain letters or engage in “spamming” (sending annoying, unnecessary, or unsolicited commercial messages).
- 5) Damage, alter, disrupt, or gain unauthorized access to computers or others’ systems; e.g. use others’ passwords, trespass on others’ folders, work, or files or alter or forward email messages in a manner that misrepresents the original message or a message chain.
- 6) Give unauthorized persons access to [Archdiocese](#) systems, provide access to confidential information, or otherwise jeopardize the security of the electronic communications systems (e.g., by unauthorized use or disclosure of passwords).
- 7) Transmit confidential, proprietary, or sensitive information unless the transmission is required or concordant with the [User’s](#) job duties or assigned responsibilities.
- 8) Introduce or install any unauthorized software, virus, malware, tracking devices or recording devices onto any system.

- 9) Bypass, defeat or otherwise render inoperative any network security systems, firewalls or content filters.
- 10) Access or manipulate [Archdiocese](#) services, networks, or hardware without authorization.
- 11) Provide information about, or lists of, [Archdiocese Employees](#), [Clergy](#) or other propriety information from the [Archdiocese's](#) database(s) to outside parties. Certain exceptions to this prohibition may be made with approval from the Chief Operating Officer. Use AI to generate deceptive or malicious content.

V. CONSEQUENCES OF VIOLATIONS OF ELECTRONIC COMMUNICATIONS POLICY

Violations of this policy may result in suspension of electronic communication privileges, confiscation of any electronic devices or materials, and imposition of discipline, up to and including termination of employment or referral for canonical review.