ACCEPTABLE USE AND RESPONSIBILITY POLICY FOR ELECTRONIC COMMUNICATIONS
[“ARCHDIOCESAN AUP”]
2022-2023

All information used in the course of activities for or on behalf of the Roman Catholic Archdiocese of Los Angeles ("Archdiocese") or an archdiocesan school, parish, the seminary, a cemetery, or other archdiocesan department or operating unit (“Location”) is an asset of the Archdiocese and/or the Location, as appropriate. Electronic information and communications require particular safeguards and impose unique responsibilities on all users. The Archdiocese maintains a system of information security to protect our 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 for the complete system to remain viable.

These policies, standards and procedures apply to all users of technology, whether adult, child or youth, whether they are paid or volunteer staff, clergy or members of religious orders, in the Archdiocese or in any Location.

These policies, standards and procedures include, but are not limited to, 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 archdiocesan data and/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.

Definitions

Electronic communications systems include, but are not limited to, electronic mail, telecommunications systems including telephone, voice mail, and video, facsimile transmissions, stand-alone or networked computers, intranets, the Internet and any other communications systems that may be created in the future.
Electronic communications devices include, but are not limited to, regular and mobile telephones (cell phones, smart phones, walkie-talkies), facsimile machines, computers, laptops, electronic notebooks, audio and video equipment, flash drives, memory sticks, iPods®, media players, Blackberries®, and other wireless equipment that may be created in the future.

Electronic communications materials include, but are not limited to, DVDs, CDs, laser discs, audio and video-tape, audio and visual recordings, films, microfiche, audio and visual broadcasts, computer operating systems, software programs, electronically stored data and text files, computer applications, emails, text

messages, instant messages, and all other downloaded, uploaded, retrieved, opened, saved, forwarded or otherwise accessed or stored content.

Electronic Communications Systems, Devices and Materials and Users Covered

a. All electronic communications systems, devices and materials in the schools, parishes, the seminary, cemeteries, archdiocesan departments or offices, or other archdiocesan operating units (the "Premises").
b. All electronic communications devices and materials taken from the Premises for use at home or on the road.
c. All personal devices and materials brought from home and used on the Premises during regular business hours.
d. All personal devices and materials, regardless of where they are situated, that are used in such a manner that the Archdiocese and/or the Location may be implicated in their use
e. All users of electronic communications systems, devices and materials, including, but not limited to, volunteers, clergy and religious, students, employees, staff or contractors associated with the Archdiocese and/or the Location.

Ownership and Control of Communications

All systems, devices and materials located on archdiocesan premises, and all work performed on them, are property of Location and/or the Archdiocese. These systems, devices and materials are to be used primarily to conduct official Location and/or Archdiocese business, not personal business.

With permission from the person in charge of the parish (i.e., pastor, priest administrator or parish life director), principal or other person in charge of the Location, individuals may use systems, devices and materials, including access to the Internet, for personal business and web exploration outside regular business hours or during breaks. All users are expected to conform to appropriate content management and web surfing guidelines, whether during or outside regular business hours.

The Archdiocese and the Locations, as applicable, reserve the right to monitor, access, retrieve, read and disclose all content created, sent, received, or stored on Archdiocese and/or Location systems, devices and materials (including connections made and sites visited) to law enforcement officials or others, without prior notice.

Guidelines for Email Correspondence and Other Electronic Communications

a. All users of Archdiocese and Location communications systems and devices should use care in creating email, text, video, still images, instant or voice mail messages or in any postings on any social networking site. Even when a message has been deleted, it may still exist on a backup system, be restored, downloaded, recorded, printed out, or may 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 cannot be considered private or confidential.
b. Email and other electronic communications are not necessarily secure.
c. As with paper records, proper care should be taken in creating and retaining electronic records for future use, reference and disclosure, as applicable.
d. Postings to "All Employees," "All Parents," "All Seminarians," "All Parishioners" and the like on intranets or the Internet must be approved by the person in charge of the parish (pastor, priest administrator or parish life director), principal or other person in charge of the Location before they are sent out.
e. Use of personal electronic communications devices and materials during regular business hours should be kept to a minimum and limited mainly to emergencies.
f. Archdiocese and Location 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 account passwords for systems not controlled by a centralized user

directory or authentication system must be on record with the person in charge of the parish (pastor, priest administrator or parish life director) principal or other person in charge of the Location.

g. User IDs and passwords should not be disclosed to unauthorized parties or shared with other employees, students or volunteers. User accounts are intended to be used only by the assigned party.
h. All information systems that create, store, transmit or otherwise publish data or information must have authentication and authorization systems in place to prevent unauthorized use, access, and modification of data and applications. Systems that transmit or publish approved information that is intended for the general public may allow unauthenticated (anonymous) access as long as such systems do not allow unauthorized posting and modification of the published information.
i. Any device accessed or used by minors on the Premises must include updated and functioning filters to preclude access to prohibited content. All obscene materials, sexually explicit materials including pornography, and materials that are otherwise harmful to minors or in violation of this electronic communications policy are prohibited and must be blocked. Before allowing minors to access the Internet, a responsible adult must ensure that appropriate content filters are "ON" and functioning.
j. Content filters for minors may NOT be disabled or turned "OFF" without obtaining prior permission from the archdiocesan Applied Technology Department or the person with equivalent authority at the location.
k. All files downloaded from the Internet, all data received from outside sources, and all content downloaded from portable memory devices must be scanned with updated or current virus detection software. Immediately report any viruses, tampering or other system breaches to the person in charge of the location.
l. Critical information should be copied onto backup storage periodically. Backed up information should be stored in a safe place and be available for recovery in case of a loss of the original information. Depending on the complexity of a Location's information systems, a detailed disaster recovery plan may need to be developed.
m. Computer networks must be protected from unauthorized use. Both local physical access and remote access must be controlled.
n. Information systems hardware should be secured against unauthorized physical access.

Prohibited Practices

Users of Archdiocese and Location electronic communication systems, devices or materials and users of personal devices and materials on the Premises under circumstances when the Archdiocese and/or the Location may become implicated in the use may not:

a. Violate any federal, state or local laws or regulations.
b. Violate any rules of conduct, codes of ethics, safe environment or any educational policies, including but not limited to those that apply to communications or the use of information.
c. Post or cause to be distributed any personally identifying information about the user or others without permission or review by a responsible adult person, unless required by the user's job duties or assigned responsibilities. Personal identifying information includes, but is not limited to, names or screen names; telephone numbers; work, home or school addresses; email addresses and web addresses (URLs) of social networking sites or blogs.
d. Post or distribute any communications, video, music or pictures which a reasonable person, according to the teachings of the Roman Catholic Church, would consider to be defamatory, offensive, harassing, disruptive, derogatory or bullying. This includes, but is not limited to, sexual comments or images, racial or ethnic slurs, or other comments or images that would offend someone on the basis of race, creed, gender, national origin, sexual orientation, age, political beliefs, mental or physical disability, or veteran status.
e. Engage in improper fraternizing or socializing between adults and minors.

f. Engage in pirating or unauthorized copying, acquisition or distribution of copyrighted materials, music, video or film; arrange for the purchase or sale of any drugs, alcohol, or regulated substances and goods; or participate in internet gambling.
g. Post or send chain letters or engage in "spamming" (sending annoying, unnecessary or unsolicited commercial messages).
h. Record any telephone, video, or other conversation or communication without the express permission of the other participants to the conversation or communication, except where allowed by law.
i. Use electronic communications devices for designing, developing, distributing or storing any works of programming or software unless required by the duties of the job or assignment.
j. Upload, download, view or otherwise receive or transmit copyrighted, trademarked, patented, indecent or pornographic material, 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. See *Archdiocese of Los Angeles Copyright and Video Screening Policy*.
k. Damage, alter, disrupt, or gain unauthorized access to computers or other 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.
l. Give unauthorized persons access to Archdiocese or Location 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).
m. Transmit confidential, proprietary, or sensitive information unless the transmission falls within the scope of the user's job duties or assignment by a responsible adult.
n. Introduce or install any unauthorized software, virus, malware, tracking devices or recording devices onto any system.
o. Bypass (via proxy servers or other means), defeat or otherwise render inoperative any network security systems, firewalls or content filters.
p. Allow any minor to access the Internet on Archdiocese or Location communications devices before a responsible adult has checked to insure that active filtering of prohibited materials is enabled.
q. Use electronic communications devices or systems to transmit any radio frequency signal that is not permitted and/or licensed by the Federal Communication Commission ("FCC") or that would violate FCC rules or policies.
r. Access or manipulate services, networks or hardware without express authority.

Consequences of Violations of Electronic Communications Policy

Violations of this policy, including breaches of confidentiality or security, may result in suspension of electronic communication privileges, confiscation of any electronic communication device or materials, and disciplinary action up to and including termination of employment, removal from parish or school activities, expulsion from school, canonical review, referral to law enforcement and other appropriate disciplinary action.