ACCEPTABLE USE AND RESPONSIBILITY POLICY FOR ELECTRONIC COMMUNICATIONS (“ARCHDIOCESAN AUP”)

All information created and used in the course of activities for or on behalf of the Roman Catholic Archdiocese of Los Angeles ("Archdiocese") or an archdio cesan school , a parish, the seminary, a cemetery , the Archdiocesan Catholic Center , or another 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 its 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 adults, children, or youth and 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 communication **systems** include but are not limited to email, telecommunications systems (including telephone, voice mail, and video), stand-alone or networked computers, intranets, the Internet, and any other communication or data transmission systems that may be created in the future.

Electronic communication **devices** include but are not limited to regular and mobile telephones, two-way radios, facsimile machines, computers, laptops, electronic notebooks, tablets, audio and video equipment, flash drives, memory sticks, media players, and other communications equipment that may be created in the future.

Electronic communication **materials** include but are not limited to DVDs, CDs, laser discs, audiotape and videotape, audio and visual recordings, films, microfiche, audio and visual broadcasts, computer operating systems, software programs, electronically stored data and text files, computer and web applications, emails, text messages, instant messages, and all other electronic content that is downloaded, uploaded, retrieved, opened, saved, forwarded, or otherwise accessed or stored.

Person in charge refers to the department head, manager, or supervisor of an archdiocesan department, entity, or corporation; the pastor, parish life director, pastoral

associate, or parish business manager; or the superintendents of elementary schools or high schools, a supervisor in the Department of Catholic Schools, a principal, or a president or head of school, as applicable.

Location refers to an archdiocesan school, a parish , the seminary , a cemetery, the Archdiocesan Catholic Center, or another archdiocesan department or operating unit.

Electronic Communication Systems, Devices, and Materials and the Users Covered

Electronic communication systems, devices, and materials and the users covered include:

- All electronic communication systems, devices, and materials in the schools , pa rishes, seminary , cemeteries, archdiocesan departments or offices, or other archdiocesan operating units (the "Premises")
- All electronic communication devices and materials taken from the Premises for use at home or on the road
- All personal devices and materials brought from home and used on the Premises during regular business hours
- 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
- All users of electronic communication 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 electronic communication systems, devices, and materials located on archdiocesan premises, and all work performed on them, are the property of the 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 Location, individuals may use archdiocesan systems, devices, and materials to access and use the Internet for personal business and web exploration outside regular business hours or during breaks. All users shall conform to appropriate content management and web surfing guidelines, whether during or outside regular business hours.
The Archdiocese and 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.

Internet Safety Policy

Any device accessed or used by minors on the Premises must use functioning and properly configured content filters to preclude access to prohibited content, including obscene, sexually explicit materials; adult or child pornography; and materials including applications that are otherwise harmful to minors or in violation of this Archdiocesan AUP .
Content filters for minors may NOT be disabled or turned off without obtaining prior permission from the archdiocesan Department of Applied Technology or the person with equivalent authority at the Location.
No unauthorized personal identification information regarding minors may be disclosed, used, or disseminated without proper authorization by a responsible person at the Location.
Minors' use of email, chat rooms, social networks, applications, and other forms of direct electronic communication on electronic devices at the Location must be monitored.
No person may engage in unlawful activities online, including hacking archdiocesan or Location systems or any system while using Archdiocese or Location devices or while on the Premises of any Location.

Prohibited Practices

Users of Archdiocese and or 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:

- Violate any rules of conduct, codes of ethics, or safe environment or any educational policies, including but not limited to those that apply to communications or the use of information
- Host any website on a domain that is not owned by the Archdiocese or, if the domain is owned by a third party, is not under contract with the Archdiocese
- Use the name, logo, identifying photograph, mission statement, or other singularly identifying information of the Archdiocese or a Location on a website or other social medium in such a manner that readers/viewers are lead to believe that the website or social medium is an official site or medium controlled by the Location itself
- Post or cause distribution of any personally identifying information about the user or others without permission of 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; or web addresses/ URLs of social networking sites or blogs)
- Post or distribute any communications, videos, music, or pictures that a reasonable person, according to the teachings of the Roman Catholic Church, would consider to be defamatory, offensive, harassment, disruptive, derogatory, or bullying; these include but are 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

- Engage in improper fraternizing or socializing between adults and minors
- Engage in cyberbullying or other abusive online behavior
- Engage in pirating or unauthorized copying, acquisition, or distribution of copyrighted materials, music, videos, or film
- Post or send chain letters or engage in spamming (sending annoying, unnecessary, or unsolicited commercial messages)
- Record any telephone, video, or other conversation or communication without the express permission of the other participants in the conversation or communication, except where allowed by law
- 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 the Archdiocese of Los Angeles Copyright and Video Screening Policy)
- Damage, alter, disrupt, or gain unauthorized access to computers or other systems (e.g., use another person's passwords; trespass on another person's folders, work, or files; or alter or forward email messages in a manner that misrepresents the original message or message chain)
- Give unauthorized persons access to Archdiocese or Location systems, provide access to confidential information, or otherwise jeopardize the security of the electronic communication systems (e.g., by unauthorized use or disclosure of passwords)
- Transmit confidential, proprietary, or sensitive information unless the transmission falls within the scope of the user's job duties or the assignment as given by a responsible adult
- Introduce or install any unauthorized software, virus, malware, tracking devices, or recording devices onto any system
- Bypass (via proxy servers or other means), defeat, or otherwise render inoperative any network security systems, firewalls, or content filters
- Allow any minor to access the Internet on Archdiocese or Location communication devices without active, monitored filtering of prohibited materials
- Allow any minor to use email, chat rooms, social networking sites, applications, or other forms of direct communications at the Location without monitoring
- Use electronic communication devices or systems to transmit any radio frequency signal that is not permitted and/or licensed by the Federal Communications Commission (FCC) or that would violate FCC rules or policies
- Access or manipulate services, networks, or hardware without express authority
- Violate any other applicable federal, state, or local laws or regulations

Consequences of Violations of the 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 local or other law enforcement, and other appropriate disciplinary action.

Guidelines for Email Correspondence and Other Electronic Communications

All users of Archdiocese and Location communication systems and devices should use care in creating email, text, video, still images, instant or voice mail messages, or any postings on any social networking site. 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. The contents of email and text messages are the same as other written documentation and cannot be considered private or confidential.

Email, texts, and other electronic communications are not necessarily secure.

As with paper records, proper care should be taken in creating and retaining electronic records for future use, reference, and disclosure, as applicable. See Document Retention.

Postings to "All Employees," "All Parents/Guardians," "All Seminarians," "All Parishioners," and the like on intranets or the Internet must be approved by the person in charge of the Location before the postings are sent out.

Use of personal electronic communication devices and materials during regular business hours should be kept to a minimum and limited mainly to emergencies.

Archdiocese and Location systems, devices, and materials are not private and security cannot be guaranteed. User IDs and passwords are intended to enhance system security, not to provide users with personal privacy. User account passwords for systems that are not controlled by a centralized user directory or authentication system must be on record with the person in charge of the Location.

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.

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.

All files downloaded from the Internet, all data received from outside sources, and all content downloaded from portable memory devices must be scanned with current virus detection software. Immediately report any viruses, tampering, or other system breaches to the person in charge of the Location.

Critical information should be periodically copied onto backup storage. Information that is backed up 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.
Computer networks must be protected from unauthorized use. Both local physical access and remote access must be controlled.
Information systems hardware should be secured against unauthorized physical access.