

§800 ELECTRONIC COMMUNICATIONS

The Archdiocese of Chicago provides and uses many forms of communication and information technologies. These technologies, when properly used, support our business and pastoral activities and enable closer and timely communication within the Archdiocese and with our constituents. There is a continuing evolution of associated laws and conventions governing acceptable use and careless use of electronic communication tools that can have dramatic consequences, harming the Archdiocese, our constituents, and our employees. These policies are intended to minimize the likelihood of such harm by educating our staff and by acting as the basis for written policies and procedures whose existence will serve to protect the Archdiocese in litigation and other disputes. Access to Archdiocesan communications tools is provided in conjunction with the Archdiocese's business and staff job responsibilities. Staff use of these tools is subject to this policy and other Archdiocesan policies and procedures. This policy is binding for all Archdiocesan Staff. Archdiocesan communication tools also may be made available to individuals who are not Archdiocesan staff (e.g., consultants, vendors, committee members, temporaries, and volunteers). Use of these tools by such persons is subject to this policy.

§801 USE AND MISUSE OF COMMUNICATION TOOLS

DEFINITION:

“Communication tools” include, but are not limited to, E-mail, Internet, Computers, and Voicemail.

§801.1. OWNERSHIP AND ACCESS

801.1.1. Policy Communications tools purchased or provided by the Archdiocese for use in the performance of its business are Archdiocesan property and subject to reasonable inspection. All information created in the course of Archdiocesan business and/or produced or carried on Archdiocesan communications tools is likewise Archdiocesan property and subject to reasonable inspection.

801.1.2. Policy Each user accessing these tools must have a unique user ID assigned by the system administrator. Under no circumstances shall it be permissible to allow another person to use one's ID or password.

§801.2. ACCEPTABLE USE

In the course of their employment, staff may use these tools to communicate internally with Archdiocesan coworkers or externally with parishes, agencies, consultants, vendors, and other professional and business acquaintances. The Archdiocese provides staff with electronic communication tools to facilitate business communications and to enhance productivity.

801.2.1. Policy As with the telephone, there may be occasion to use these communication tools for personal purposes. Personal use is permitted so long as it does not interfere with the job performance, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other staff members.

801.2.2. Policy Under no circumstances shall such communication tools be used for personal gain, or to solicit others for activities unrelated to the Archdiocese's business, or in connection with political campaigns or lobbying.

Procedures

- a) Human Resources may make available or otherwise authorize use for Archdiocesan-approved social events or other sanctioned activities.
- b) When making use of these Archdiocesan-provided facilities for personal use, staff should be mindful that there is a very limited expectation of privacy.

801.2.3. Policy Staff may not use any communication tool:

- (1) to carry defamatory, discriminatory, or obscene material;
- (2) to infringe upon another person's intellectual property rights (e.g. copyrights);
- (3) in a manner that violates the terms of any applicable telecommunication license or any laws governing transborder data flow (e.g., laws dealing with data collection, protection, privacy, confidentiality, and security); or
- (4) in connection with any attempt to penetrate computer or network security of any company or other system, or to gain unauthorized access (or attempted access) to any other person's computer, email or voicemail accounts or equipment: or in connection with the violation or attempted violation of any other law.

§801.3. INTERNET USE

The Archdiocese is aware that web “surfing” may be business-related and serve a legitimate business function, but the potential for abuse exists. The Internet provides access to a huge amount of information and resources that can greatly enhance our ability to deliver services to our constituents. Today there is no single, comprehensive directory of resources available for the Internet and users sometimes must “navigate” through much unneeded information to reach useful material.

801.3.1. Policy The Archdiocese encourages exploration of the Internet for legitimate business-related or professional activities, but staff shall not “browse the web” on Archdiocesan time, create personal “Home Pages”, or otherwise use Archdiocesan facilities to access Internet sites for reasons unrelated to Archdiocesan business and staff job responsibilities.

§801.4. REPRESENTING THE ARCHDIOCESE IN STAFF POSTINGS

Any information published electronically (sometime called a “Posting”) is a reflection on the Archdiocese of Chicago. Despite disclaimers that may be made (e.g., that views belong to a particular individual and may not reflect those of the Archdiocese) readers elsewhere may make the association between a posting and the Archdiocese of Chicago. Staff should be aware that true anonymity is very difficult to obtain when using these tools. While Internet relay chat (“IRC”), newsgroup visits, and net “surfing” sometimes appear to be done anonymously (e.g., by employing pseudonyms), accessing such services/servers through the Archdiocese’s network facilities normally leaves an “audit trail” indicating at least the identity of the Archdiocese’s proxy/server (and may leave an audit trail pointing directly to an individual). Inappropriate use of Archdiocesan facilities may damage the Archdiocese’s reputation and could give rise to corporate and individual liabilities.

801.4.1. Policy Staff shall make every effort to be professional in all usage of Archdiocesan communication tools and ensure that information is correct before posting any article or opinions.

801.4.2. Policy Staff shall use a disclaimer that the opinions offered are their own and do not necessarily reflect the opinions or position of the Archdiocese of Chicago.

§801.5. UNACCEPTABLE CONTENT

Although the Archdiocese does not regularly monitor voicemail or electronic messages, staff should be aware that even personal mail and voicemail messages may be viewed publicly or by Archdiocesan management without further notice.

801.5.1. Policy Under no circumstances shall any posting, voicemail or email originating at the Archdiocese be in violation of the teachings of the Catholic Church, the letter or spirit of the Archdiocese's Equal Employment Opportunity or Sexual Harassment policies, or the restrictions against 501(c)(3) tax exempt organizations (cf. *Political Responsibility: Proclaiming the Gospel of Life, Protecting the Least Among Us, and Pursuing the Common Good*, United States Catholic Conference, 1995.). Examples of unacceptable content include, but are not limited to:

- (1) sexually explicit messages, images, cartoon or jokes;
- (2) unwelcome propositions, requests for dates, love letters, profanity, obscenity, slander, or libel;
- (3) direct or indirect support for or opposition to any candidate for elective public office;
- (4) distribution of campaign literature or biased voter educational material;
- (5) publication or transmission of paid political advertising, biased coverage of candidate activity or opinions that endorse or oppose a particular candidate;
- (6) endorsements of candidates or political parties;
- (7) ethnic, religious, or racial slurs; or
- (8) any message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious beliefs.

The standard used to determine whether or not "sexual harassment" has occurred is whether the recipient could reasonably consider the message to be offensive - - the sender's intentions are irrelevant.

§801.6. ELECTRONIC FORGERY

Electronic forgery is defined as misrepresentation of identity in any way while using electronic communication systems (e.g., by using another's email account without permission, or so-called IP spoofing, or by modifying another's messages without permission).

801.6.1. Policy Messages written by others shall be forwarded “as-is” and with no changes, except to the extent that staff clearly indicates where they have edited the original message (e.g., by using brackets [] or by using other characters to flag edited text).

§801.7. INTELLECTUAL PROPERTY

801.7.1. Policy Staff must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and intentions. Staff may not copy use, or transfer others' materials without appropriate authorization.

Procedure

Staff are responsible for being aware that download software and other copyrighted material may be subject to licensing obligations or restrictions. When staff are in doubt, they should contact the Office of Legal Services.

§801.8. ENCRYPTION

801.8.1. Policy Archdiocesan security standards and policies also govern the use of encryption tools. Only authorized encryption tools (software and hardware) may be used in connection with any Archdiocesan communication tools. Except with the prior written consent of the appropriate IT manager, all such tools must implement key-recovery or key-escrow techniques to permit the Archdiocese to access and recover all encrypted information (e.g., in the case of the absence of the staff member who performed the encryption).

§802 LIMITS OF PRIVACY

No electronic communications facility is completely secure. This means that information stored on or carried over Archdiocesan communications tools may be the subject of accidental or intentional interception, misdelivery, attack, or authorized Archdiocesan review. When stored on computers, email messages and other files typically are subject to routine back-up procedures. This means that copies of these files may be retained for long periods of time (in accordance with back-up recycling and document retention procedures). Also, keep in mind that many site-wide backup systems do not guarantee privacy of backup copies (e.g., system administrators may have access).

§802.1. RETENTION AND SECURITY OF MESSAGES

<p>802.1.1. Policy Email and voicemail messages, and computer stored items are Archdiocesan property and business records, and may have legal and operational effect identical to that of traditional, hardcopy documents (for example, that are “discoverable” in litigation, and can be used in evidence). Retention of voice mail logs and email are governed by Archdiocesan Retention Schedules as outlined in the Archdiocesan Records Policy. Accordingly, all email messages shall be treated as though others may later view them. Email should <i>not</i> be considered a confidential means of correspondence. Staff shall employ other methods of communication for documents that may contain confidential information.</p>
--

§802.2. LIMITED EXPECTATION OF PRIVACY

The Archdiocese of Chicago respects the personal privacy of its staff. However, because communications tools are provided for *the Archdiocese’s business purposes, staff rights of privacy in this context are quite limited. Staff and other should have no expectation that any information transmitted over Archdiocesan facilities or stored on Archdiocesan-owned or leased computers is or will remain private. These systems are owned and/or controlled by the Archdiocese of Chicago and are accessible at all times by the Archdiocese for maintenance, upgrades, or any other business or legal purpose. Staff members who use Archdiocesan communication tools should be aware that our firewall (and other security tools) creates an audit log detailing every request for access in either direction by each user. Also, in the course of their duties, system operators and managers may monitor employee use of the internet or review the contents of stored or transmitted data.*

802.2.1. Policy The Archdiocese of Chicago permits limited personal use of all these communications tools on the express understanding that it reserves the right (for its business purposes or as may be required by law) to review staff use, and to inspect all material created by or stored on, these communication tools. Use of these tools constitutes the employee's permission for the Archdiocese to monitor communications and to access files that are made on or with these communication tools.

802.3. ARCHDIOCESAN ACCESS TO COMPUTERS, VOICEMAIL AND EMAIL SYSTEMS

802.3.1. Policy Archdiocesan management will not routinely examine staff communications or files. However, such examination generally may be expected to occur in the following circumstances (which are not intended to be all-inclusive):

- (1) ensuring that Archdiocesan systems are not being used to transmit discriminatory or offensive messages, or in connection with the infringement or violation of any other person's rights;
- (2) determining the presence of illegal material or unlicensed software;
- (3) counteracting theft or espionage;
- (4) ensuring that communications tools are not being used for inappropriate purposes;
- (5) responding to legal proceedings that for producing electronically-stored evidence;
- (6) locating, accessing, and retrieving information in an employee's absence; and
- (7) investigating indications of impropriety.

§803 PENALITIES

803.1. Policy Violations of these policies can result in responses ranging from denial of future access to termination of employment.