Electronic Communications Policy

Introduction

The Archdiocese of Chicago is a user of many communications 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 and guidelines are intended to minimize the likelihood of such harm by educating our employees and by acting as the basis for written policies and procedures whose existence will serve to protect the Archdiocese in litigation and other disputes

1. Use and Misuse of Communication Tools[1]

1.1 Ownership and Access

Access to Archdiocesan communications tools is provided in conjunction with the Archdiocese's business and your job responsibilities. Your use of these tools is subject to this policy and other Archdiocesan policies and procedures. This policy is binding for all Archdiocese staff members. Archdiocesan communication tools also may be made available to individuals who are not Archdiocesan employees (e.g., consultants, vendors, committee members, temporaries). Use of these tools by such persons is subject to this policy.

Additionally, each user accessing these tools MUST have a unique user id assigned by the Office of Information Technology. Under no circumstances will it be permissible to allow another person to use your id or password.

> Communications tools and all messages produced or carried by such tools are Archdiocesan property, subject to reasonable Archdiocesan inspection.

---

[1] Communication tools are defined as, but not limited to: Email, Internet, Computers, Voicemail, etc.

1.2   Acceptable Use

In the course of your job, you may use these communications tools to communicate internally with Archdiocesan coworkers or externally with parishes, agencies, consultants, vendors, and other professional and business acquaintances. The Archdiocese provides you with electronic communication tools for business communications and to advance the mission of the Archdiocese. As with the telephone, there may be occasion to use these facilities for personal purposes. Limited Personal use is permitted so long as it does not interfere with the performance of your job, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other employees. Under no circumstances shall such facilities 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. The Human Resources Department may make available or otherwise authorize use for Archdiocesan-approved social events or other sanctioned activities. When making use of these Archdiocesan-provided facilities for personal use, always remember that you have very limited expectation of privacy.

> You may not use any communication tool:
> - to carry an defamatory, discriminatory, or obscene material:
> - to harass another group or individual
> - in conjunction with any infringement of other person's intellectual property rights (e.g. copyrights);
> - 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);
> - 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

The Archdiocese understands 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 not single, comprehensive directory of resources available for the internet and users sometimes must "navigate" through much unneeded information to reach useful material.

> The Archdiocese encourages exploration of the internet for legitimate business-related or professional activities, but you must avoid "browsing the web" on Archdiocesan time, creating personal "Home Pages", or otherwise using Archdiocesan facilities to access internet sites for reasons unrelated to Archdiocesan business and your job responsibilities.

1.3   Representing the Archdiocese in Your Postings

The information you publish electronically (sometime called a "Posting") reflects on the Archdiocese in general. Despite all disclaimers that you make (e.g., that your views are your own and may not reflect those of your employer) readers elsewhere will make the association between your posting and the Archdiocese of Chicago. You should know that true anonymity is very difficult to obtain when using these tools. While internet relay chat ("IRC"), newsgroup visits, and net "surfing" sometimes appears 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 you). Inappropriate use of Archdiocesan facilities may damage the Archdiocese's reputation and could give rise to corporate and individual liabilities.

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

> You shall use a disclaimer that the opinions offered are your own and do not necessarily reflect the opinions or position of the Archdiocese of Chicago.

1.4   Unacceptable Content

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

> Under no circumstances may any posting, voicemail or email originating at the Archdiocese be in violation of the letter or spirit of the Archdiocese Equal Employment Opportunity or Sexual Harassment policies.
> Examples of unacceptable content include:
> - sexually explicit messages, images, cartoon or jokes;
> - unwelcome propositions, requests for dates, or love letters;
> - profanity, obscenity, slander, or libel;
> - ethnic, religious, or racial slurs;
> - political beliefs or commentary;
> or any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political beliefs. The standard to sexual harassment is whether the recipient could reasonably consider the message to be offensive - - the sender's intentions are irrelevant.

1.5   Electronic Forgery

Electronic forgery is defined as misrepresenting your 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).

> Messages written by others should be forwarded "as-is" and with no changes, except to the extent that you clearly indicate where you have edited the original message (e.g., by using brackets [ ] or by using other characters to flag edited text).

1.6   Intellectual Property

The internet offers a universe of information, useful in conducting and furthering business operations.

> You must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and intentions. Do not copy, use, or transfer others' materials without appropriate authorization. Be aware that download software and other copyrighted material may be subject to licensing obligations or restrictions. When there is doubt contact the office of Legal Services.

1.7   Encryption

> 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 employee who performed the encryption).

2.0 Limits of Privacy

2.1 Retention and Security of Messages

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).

> 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 they may later be viewed by others. **Email should *not* be considered a confidential means of correspondence. Employ other methods of communication for documents that may contain confidential information.**

2.2 A Limited Expectation of Privacy

The Archdiocese of Chicago respects the personal privacy of its employees. However, because communications tools are provided for the Archdiocese's business purposes, employee rights of privacy in this context are quite limited. Employees 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. Employees 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. Types, destinations, frequency and file names of web-based transactions will be logged and distributed monthly to department directors to allow them to ensure compliance with these policies. 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.

> **The Archdiocese of Chicago permits limited personal use of all these communications tools with the express understanding that it reserves the right (for its business purposes or as may be required by law) to review employee use of, 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**.

2.3   Archdiocesan Access to Computers, Voicemail and Email Systems

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

- 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;
- determining the presence of illegal material or unlicensed software;
- counteracting theft or espionage;
- ensuring that communications tools are not being used for inappropriate purposes;
- responding to legal proceedings that require producing electronically-stored evidence;
- locating, accessing, and retrieving information in an employee's absence; and
- investigating indications of impropriety.

2.4   Penalties

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