General Policy and Procedure on Technology

Prepared by the Office of Information Technology

April 2010
(Adopted by Administrative Council June 7, 2010)

INTRODUCTION

The Roman Catholic Church of the Archdiocese of New Orleans provides and uses many forms of communication and information technologies. These technologies, when properly used, support our ministries and pastoral activities and enable closer and timely communication within the Archdiocese. There is a continuing evolution of associated laws and conventions governing acceptable use and careless use of electronic communication tools that can have consequences, possibly harming the Archdiocese and employees of the Archdiocese. These policies are intended to minimize the likelihood of such consequences by educating users and by acting as the basis for written policies and procedures whose existence will help protect the Archdiocese and its employees. Access to Archdiocesan communication tools is provided in conjunction with the Archdiocese's ministries and the user's job responsibilities. A user of these tools is subject to this policy and other Archdiocesan policies and procedures. This policy is binding for the Archdiocese and all Archdiocese users[1]. Archdiocesan communication tools also may be made

available to individuals who are not of the Archdiocese (e.g., consultants, vendors, committee members, temporaries, and volunteers). Use of these tools by such persons when allowed is also subject to this policy.

Ownership and Access

> *Communication tools[2] and network-related systems[3] purchased or provided by the Archdiocese for use in the performance of its ministries are the Archdiocese's property and subject to reasonable inspection. All information created in the course of the Archdiocese's ministries and/or produced or carried on Archdiocesan communication tools is likewise Archdiocesan property and subject to reasonable inspection. These systems are to be used for purposes in serving the interests of the Archdiocese. No person is expressly, implicitly or otherwise authorized to use the property of the Archdiocese for excessive personal use or outside of the scope of these Policies.*

Individual users shall be aware that the data they create on these systems remains the property of the Archdiocese or its related entities. Accordingly, no individual should have any expectation of privacy in respects to the content or data contained on his or her network related systems.

Use and Misuse of Communication Tools

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

Each user accessing these tools must have a unique user ID assigned by the system administrator. All accounts must have a password equal to or exceeding the password security guidelines promulgated by the Archdiocesan Office of Information Technology. Under no circumstances shall it be permissible to allow another person the use of one's ID or password. ***All passwords must be treated as sensitive and confidential Archdiocesan proprietary information.***

1) Mobile Computing & Storage Devices

With advances in computer technology, mobile computing and storage devices[4] have become useful tools to meet needs. These devices are especially susceptible to loss, theft, hacking, and the distribution of malicious software because they are easily portable and can be used anywhere.

All mobile computing and storage devices containing or accessing information resources must be approved by the Office of Information Technology and/or their delegates prior to connecting to Archdiocesan information systems.

Any and all users of mobile computing and storage devices must diligently protect such devices

from loss of equipment and disclosure of private information belonging to or maintained by the Archdiocese.

2) Remote Access

Remote access to Archdiocesan network resources is achieved using a high security two-factor authentication system utilizing hardware token authenticators. Written approval from an Office Director or appropriate Supervisor as well as final approval from the Office of Information Technology is required to utilize this resource,

a) *It is the responsibility of Archdiocesan employees, contractors, vendors and agents with remote access privileges to the Archdiocese's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Archdiocese. The user must ensure that their Archdiocesan-owned or personal computer or workstation that is remotely connected to the Archdiocesan corporate network is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.*

b) *All hosts that are connected to Archdiocesan internal networks via remote access must use the most up-to-date anti-virus software and definitions, if applicable. This includes personal computers.*

c) *General access to the Internet for recreational use by Archdiocesan employees and household members through the Archdiocesan Network on personal computers is strictly prohibited. The employee bears responsibility for all consequences if remote access is misused.*

3) Unacceptable Use

The following activities are deemed "unacceptable uses," in general, and are therefore prohibited:

a) *Illegal activities under local, state, federal or international law including: (1) downloading of video and music in violation of copyright laws, (2) unauthorized copying of copyrighted material, including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, (3) installing of any copyrighted software for which the Archdiocese or related entity does not have an active license, or (4) using software files, images or other information downloaded from the Internet that has not been released for free publication.*

b) *Locations that have minors shall not have access to any Internet sites or materials that violate any policies of the Archdiocese, including but not limited to Safe Environment, Children's Internet Protection Act (CIPA), or any other applicable laws that govern the use of technological tools by minors.*

c) *Transmissions that violate copyrights held by others; transmission of threatening,*

violent, or obscene material; or transmissions that contain inappropriate language.

d) *The posting or distribution of any communications, video, music, or pictures which a reasonable person would find contrary to the morals and teachings of the Roman Catholic Church or any policies of the Archdiocese of New Orleans or which would be considered 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, age, political beliefs, mental or physical disability, or veteran status.*

e) *Acts of vandalism as defined as any malicious attempt to harm or destroy data of another user or to damage hardware or software or system or network activities. This includes, but is not limited to, the uploading or creation of computer viruses or introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, or e-mail bombs.)*

f) *Unauthorized use of another individual's computer, access accounts, and/or files.*

g) *Use of non-Archdiocesan Internet access that allows a location to circumvent the Archdiocesan firewall and security devices. These connections create a "back-door" into the network resources that could compromise network security.*

h) *The following System and Network activities:*

- *Bypassing applicable security restrictions, whether or not they are built into the operating system or network, and whether or not they can be circumvented by technical means.*

- *Using an Archdiocesan computer or technology information resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.*

- *Using the technology resources of the Archdiocese to engage in other inappropriate conduct, e.g., making fraudulent offers of products, items, or services*

- *Not having up-to-date anti-virus software for hosts that will connect to Archdiocesan networks. Active anti-virus subscription on Window's systems is vital for network security*

i) *The following E-mail and Communications activities:*

- *The sending of unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).*

- *Any form of harassment via e-mail, telephone or paging, whether through language,*

frequency, or size of messages.

- *Unauthorized use, or forging, of e-mail header information.*
- *Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.*
- *The creating or forwarding of "chain letters", "Ponzi" or other "pyramid" schemes of any type.*
- *The use of unsolicited e-mail, originating from within the Archdiocesan networks, of other Internet, Intranet or Extranet service providers on behalf of, or to advertise, any service hosted by the Archdiocese or connected via the Archdiocesan network.*
- *The posting of the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).*
- *The use of the Archdiocesan logos or materials in any web page, Internet posting, or printed material, unless it has been approved in advance by the Archdiocesan Office of Communications.*
- *Any other activity that does not comply with the Archdiocesan Electronic Communications Policy.*

4) User Termination

Any user who no longer has a valid reason to access Archdiocesan property, systems and personal computer systems (whether due to termination of employment, end of assignment, or otherwise) is required to return to the Archdiocese all information regarding systems access, including, without limitation: password(s), documentation about system(s), user manuals, and any Archdiocese data or information contained on mobile computing or storage devices in his/her possession. Such users are prohibited from accessing, or attempting to access, Archdiocesan property, systems, and personal computer systems, using any method. The Archdiocese reserves the right to use all means to enforce its rights against users that violate the foregoing provisions.

Limits of Privacy

Because communication tools are provided for the Archdiocese's business purposes, users' rights of privacy in this context are limited. Users shall have no expectation that any information transmitted over Archdiocesan facilities or stored on Archdiocesan-owned computers is or will remain private. These systems are owned and/or controlled by the Archdiocese and are accessible at all times by the Archdiocese for maintenance, upgrades, or any other business or legal purpose. Users who use Archdiocesan communication tools shall be aware that the Archdiocesan 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 from the Office of Information Technology may monitor employee use of the Internet or review the contents of stored or transmitted data.

Penalties

Violations of these policies may result in responses ranging from revocation of technology resource privileges to termination of employment.

Policy and Procedure Policies On Technology

USER AGREEMENT FORM

I have received a copy of the Policy and Procedures on Technology (the "Policies") prepared by the Office of Information Technology of the Archdiocese of New Orleans, which is applicable to me through my employment with the Archdiocese or one of its affiliated entities.

*I understand that I am responsible to understand and comply with the terms of the Policies, and all policies and requirements contained therein***.**

I acknowledge that the Archdiocese of New Orleans through its Office of Information Technology may monitor and record the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive may be monitored and recorded.

*I understand that any violation of this Policy may lead to disciplinary action, including but not limited to, termination of my employment***.**

_____ _____

Signature *Date*

_____

Name (print)

_____

Title

[1] *An "Archdiocesan entity" as used herein shall include any archdiocesan department, institution, office, parish, mission, archdiocesan school, parochial school, or corporation as found in the Archdiocese of New Orleans section of the Official Catholic Directory whether separately incorporated or not. However, nothing herein shall be construed as affecting the separate corporate nature of any separately incorporated, affiliated entity, and "Archdiocese" is used for descriptive purposes only. "Archdiocesan" is descriptive of "Archdiocese." This does not apply to independent entities listed in the Official Catholic Directory under the Archdiocese of New Orleans but are recognized as Catholic organizations by the Archbishop as Shepherd of the Archdiocese.*

[2] *Communication tools include, but are not limited to E-mail, Internet, Websites, Computers, Smart (cell) Phones, Instant Messaging, and Voicemail.*

[3] *Network-related systems, including, but not limited to, computer equipment, communication devices, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfer protocols.*

[4] *Mobile computing and storage devices include, but are not limited to, the following: laptop computers, personal digital assistants (PDAs), plug-ins, Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless network cards, and any other existing or future mobile computing or storage device.*