ARCHDIOCESE OF PORTLAND IN OREGON
TECHNOLOGY POLICIES AND PROCEDURES

This policy replaces Appendix A to the
Employee Handbook for Archdiocesan Personnel **and is effective February 1, 2012**

These Technology Policies and Procedures refer to use of technology, including but not limited to computer resources of the Archdiocese of Portland in Oregon ("Archdiocese" or "Employer"), defined as Archdiocesan computers, systems, storage devices, cell phones, and other equipment/hardware as well as software, networks, websites, and other internet connections ("Archdiocesan Computer Resources").

Employees are expected to be familiar with these Archdiocesan policies and procedures; violations may result in disciplinary action, up to and including termination of employment. If you have any questions on these policies and procedures, contact the Director of Communications, Network Operations Manager, Chief Financial Officer, or Director of Human Resources.

Ownership

Archdiocesan Computer Resources are owned by the Archdiocese. As the Employer, the Archdiocese has the right to view, monitor, inspect, and/or copy — at any time and without notice —an employee's computer, accounts, files and electronic communications, including but not limited to:

- Personal and work-related files
- Software
- Downloads
- Internet and network activity
- Emails, chats and other electronic communications, including those on social media.

All materials and communications that are Archdiocesan property must be left intact upon separation from employment. The Archdiocese purchases hardware and software to be used in the normal course of business. Other hardware or software may not be installed on the network. The Network Operations Manager should be consulted about departmental needs for specialized or custom software.

Computer/Account Usage

Access to Archdiocesan Computer Resources is obtained through a login and corresponding password. Although you choose your own password, the Archdiocese retains control of all computer functions, including email and Internet access, along with the right to view and inspect all data, emails, etc.

You may access Archdiocesan Computer Resources only if explicitly authorized by the Archdiocese and primarily for job-related functions. For nonexempt employees, personal use is allowed only during lunch hours, breaks and emergencies. For exempt employees, occasional personal use is allowed so long as it is not excessive or disruptive to work priorities and responsibilities. However, all personal use of Archdiocesan Computer Resources remains subject to the terms and restrictions in this document, including the Archdiocese's right to monitor all computer and internet activity.

An employee's use of personally-owned computers and other means of electronic communication for the employee's personal use is also restricted during the work day as indicated above.

Nonexempt employees are not expected to respond to work-related emails or other electronic communications before or after normal work hours unless specifically requested to do so. Your supervisor occasionally may make such requests as work necessity requires.

Network Access

Your unique login and password must not be shared with others. Allowing another person to use your login/password to access Archdiocesan or other information and/or the internet is a serious breach of security. Report immediately to your supervisor if you suspect any unauthorized use of your login/password by another person.

Upon separation from employment, an employee will be required to provide the Network Operations Manager any passwords necessary for access to information on Archdiocesan Computer Resources.

Confidential Information

Archdiocesan policies regarding confidentiality of information apply to electronic as well as hard copy data. If confidential data pertaining to your job is lost or stolen, notify your supervisor immediately. Authorization from your supervisor is required before confidential data may be transported offsite, and it must be password protected in advance. If you inadvertently access confidential (or sensitive) data that does not pertain to your job, notify your supervisor immediately.

No email or other electronic communication, even when intended to be confidential, is totally confidential when sent electronically. Even an erased or password protected communication may be retrieved and read. Employees should mindful of this when using Archdiocesan Computer Resources.

Secure your computer when you leave it unattended, especially if you will be gone for an extended period. Log off the computer at the end of each day.

Keep all portable electronic communication devices (e.g., laptops, cell phones, etc.) in your possession or otherwise properly secured at all times.

Virus Protection

Virus protection is installed on all Archdiocesan desktop computers and is regularly updated. Laptop computers, however, may become vulnerable to viruses, and software may become outdated unless regularly connected to the server. Therefore, Employees with Archdiocesan-owned laptops should schedule regular laptop connections with the server.

Applicable Laws and Regulations

In using Archdiocesan Computer Resources, employees must comply with:

1. All relevant federal, state, and local laws, including those pertaining to libel, copyright, trademark, privacy, obscenity, and child pornography, as well as laws specific to computer, cell phone, and communication systems, such as the Computer Fraud and Abuse Act and Electronic Communications Privacy Act.
2. All relevant Archdiocesan rules and regulations, including policies in the *Employee Handbook for Archdiocesan Personnel*.
3. The Archdiocese may, and in certain circumstances must, advise appropriate law enforcement authorities of suspected illegal activities that involve Archdiocesan Computer Resources.

Use of Email

The Archdiocese provides employees with an email system to expedite necessary business communications. The email system hardware is Archdiocesan property; all messages composed, sent, or received on it are Archdiocesan property.

The Archdiocese reserves the right to examine email, personal file directories, and other information stored on or within Archdiocesan Computer Resources at any time and without prior notice. This includes monitoring the content of email.

Take care when drafting and transmitting email messages. Assume your message(s) may be received or accessed by someone other than the intended recipient, and use the same restraint and caution as when writing a letter or memo.

Transmitting Email to Large Address Groups (Archdiocesan Pastoral Center)

You may not send an email to all other employees through the **Archdiocesan Pastoral Center** or other large address group unless authorized by your supervisor. Likewise "blast" or other large group emails sent outside the Employer's network require supervisory authorization. Excessive use of such address groups may strain the Employer's network and disrupt work operations.

Laptop Use and Care

Laptops provided by the Archdiocese must be password protected before use. Confidential data on laptops must be saved to and accessed only through the Archdiocesan network. Employees with laptops should:

1. Mark the laptop and bag clearly as Archdiocesan property

2. Handle the equipment carefully
3. Keep all pieces clean and in good repair
4. Never leave the laptop visible in a car; stow it in the trunk (unless it's extremely hot or cold) or take it with you
5. Use caution to keep food and liquids away from your laptop
6. Report computer system problems that you cannot resolve to your supervisor or Network Operations Manager
7. Not loan your laptop to anyone without first clearing it through the Archdiocese's Network Operations Manager.

The laptop you have been issued is your responsibility; you may be financially accountable for any damage resulting from careless handling.

Personal Websites, Social Networks, and Weblogs

The Archdiocese permits an employee to use Archdiocesan Computer Resources to access personal websites, social networks, and weblogs during the work day, as set forth above. Nonetheless, employees utilizing such publicly viewed sites must be careful to communicate as one whose employment associates him/her with the Roman Catholic Church. Whether using Archdiocesan Computer Resources or otherwise, employees must adhere to the following rules regarding use of these media:

1. You may create, post, or access personal websites, social networks, or weblogs for personal use only in accordance with the time restrictions set forth in the Computer/Account Usage section, page 1.
2. You must establish separate sites and pages for personal and professional use. Personal social networking pages and information must not be publicized or accessible to minors with whom you associate through your work with the Archdiocese.
3. No personal (i.e., not related to work events) photographs or information should appear on any social networking site sponsored by the Archdiocese.
4. If you identify yourself as an Archdiocesan employee, state clearly that the views you express are yours alone and not intended to reflect Archdiocesan views by displaying this notice in a prominent place: "The views expressed on this (personal website/social network/weblog) are mine alone and do not necessarily reflect the views of my employer."
5. Do not reveal information that is confidential or proprietary to the Archdiocese.
6. Do not show or reproduce Archdiocesan trademarks, logos, or materials.
7. Obtain prior approval from the Director of Communications to provide a link or otherwise refer to the Archdiocesan website on your personal website, social network, or weblog.
8. Adhere to the prohibitions listed below under Prohibited Activity, item 1.
9. Acknowledge by signing the attached Receipt and Acknowledgement Form that the Archdiocese reserves the right to monitor personal websites, social networks, or weblogs created on its computers during a normal workday or on personal time.

10. You may be required to confine your personal website, social network, or weblog commentary to topics unrelated to the Archdiocese (or in certain cases, temporarily suspend that activity altogether) if the Archdiocese believes this is necessary or advisable to ensure compliance with these policies and procedures or federal or state laws.
11. Postings on these media make the information available for anyone to read; there is no right to absolute privacy, and inappropriate postings may lead to disciplinary action up to an including termination of employment.

Improper, inappropriate or excessive use of personal websites, social media or other electronic communication which result in interference with work responsibilities or productivity, breach of confidentiality, or any other uses in violation of this policy, in the sole judgment of the Employer, may result in disciplinary action, up to and including termination. Any questions about whether a personal use of these media is consistent with Archdiocesan policy should be referred to the Director of Human Resources.

Prohibited Activity

The following activities are prohibited on all Archdiocesan Computer Resources:

1. Using, transmitting, seeking, or attempting to access through any electronic medium, offensive, vulgar, suggestive, obscene, abusive, harassing, threatening, discriminatory, defamatory, or illegal language or materials. Examples include images or messages with pornography, sexual implications, racial or gender-specific slurs, or any other items that offensively address someone's age, sexual orientation, religion, national origin, disability or other protected status under applicable law. This prohibition applies to all such activities and communications whether directed to someone within or outside the Archdiocese.
2. Downloading, installing, or using software/free utilities not licensed or approved for installation by the Archdiocese. (The Archdiocese strictly adheres to all software licenses and agreements.)
3. Downloading or distributing copyrighted materials without permission from the copyright holder. All users must comply with copyright and trademark laws when working with Internet materials.
4. Revealing passwords to allow family members, friends, or others to use Archdiocesan Computer Resources. Allowing other individuals to access the Archdiocesan network and Internet makes you responsible for their actions.
5. Failing to maintain confidentiality in regard to confidential or sensitive information. This includes accessing, seeking, or transmitting without a supervisor's permission or not adequately securing any device containing confidential or sensitive data.
6. Causing disruptions to or interfering with any other computer or network, such as deliberately introducing a virus or other harmful item, including corrupted data.
7. Monitoring or intercepting any data intended for a coworker without a supervisor's permission, unless this activity is part of your normal job.
8. Deleting or removing Archdiocesan files or data in violation of Archdiocesan or departmental policy on retention of electronic data.

9. Using Archdiocesan Computer Resources during work hours for any personal activity, except in accordance with the Computer/Account Usage section on page 1.
10. Using Archdiocesan Computer Resources for any personal commercial activity, including but not limited to buying, selling, or advertising of goods or services for personal financial gain.
11. Posting or subscribing to newsgroups, online discussion boards, or email list groups using Archdiocesan Computer Resources unless specifically related to Archdiocesan business.
12. Participating in online chats unless specifically required for business purposes.
13. Creating or forwarding email spam, chain letters, or Ponzi/other pyramid schemes of any type.
14. Improper, inappropriate, or excessive use of personal websites, social media or other electronic communication that results in interference with work responsibilities or productivity, breach of confidentiality, or other violation of this policy.

Violations of any of the above prohibitions may result in disciplinary action, up to and including termination of employment.

Responsibility for losses and/or costs

An employee may be required to pay costs incurred by the Archdiocese as a result of the employee's violation of this policy, including the cost of investigating the violation.

The Archdiocese assumes no responsibility for:

1. Any damage an employee may suffer, including but not limited to loss of personal data or interruption of service
2. Obligations arising through the unauthorized use of Archdiocesan Computer Resources
3. Any unauthorized charges or costs incurred by an employee while using Archdiocesan Computer Resources.

Receipt and Acknowledgment Form

Technology Policies and Procedures

Employee Name: _____ Date:_____
(please print)

I have read and understand these policies and procedures. I understand that my use of Archdiocesan Computer Resources constitutes full acceptance of the terms and restrictions described in these policies and procedures. I also understand that violation of these policies and procedures may lead to disciplinary action, up to and including termination of employment.

I understand also that the Archdiocese may amend these policies and procedures from time to time. If I have questions about these policies and procedures, any subsequent amendments, or a related matter not covered here, I will consult the Director of Communications, Network Operations Manager, Chief Financial Officer, or Director of Human Resources.

_____ _____
Employee Name Date