



**DIOCESE OF HARRISBURG  
END-USER COMPUTING POLICY**

**DIOCESE OF HARRISBURG  
END-USER COMPUTING POLICY**

**TABLE OF CONTENTS**

<b><u>Topic</u></b>	<b><u>Page</u></b>
General.....	3
Application.....	3
Responsibilities .....	4
Enforcement and Penalties for Violation.....	6
Acquisition.....	7
Information Security .....	8
Access Control .....	8
Diocesan Network Access .....	9
Backup/Recovery .....	10
Systems Development and Maintenance .....	10
Password Management .....	10
Removable Media .....	12
Mobile Devices.....	12
Remote Access .....	13
Electronic Messaging.....	14
Internet Usage and Security.....	18
Policy on Posting of Information on the Internet .....	21
Blogging .....	22
Diocesan Web Site.....	22
Virus Protection.....	23
Signature Page .....	24
Glossary.....	Appendix A

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

### **GENERAL**

Access to computer equipment systems and networks, along with other emerging technologies and systems owned or operated by the Diocese of Harrisburg is a privilege granted to the persons named below in order to promote professional excellence, innovation, and communication that is granted by the Diocese of Harrisburg subject to certain rules, regulations, and restrictions. Such access imposes certain responsibilities and obligations and is granted subject to local, state, and federal laws, as well as the norms and Policies of the Diocese of Harrisburg. This access carries with it certain ethical and moral responsibilities and obligations. Ethical use demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation or harassment. Moral use demonstrates acting in accordance with the moral or doctrinal teachings of the Catholic Church.

### **APPLICATION**

This Policy is applicable to all individuals who access the "Diocesan Network." Also referred to as the "Diocesan System" in this document, this term specifically represents all computer equipment and access devices, information systems, software, and networks owned or operated by Harrisburg Catholic Administrative Services, Inc., or the Diocese of Harrisburg. Such individuals include the following:

- Persons employed by the Diocese of Harrisburg
- Persons employed by Harrisburg Catholic Administrative Services, Inc.
- Persons employed by corporations affiliated with the Diocese of Harrisburg, including Catholic Charities of the Diocese of Harrisburg, Inc. and Kolbe Catholic Publishing;
- Persons employed by parishes within the Diocese of Harrisburg and related schools;
- All other persons, including, but not limited to, consultants, vendors, and/or volunteers;

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

- All persons who could access the "Diocesan Network" information systems via any computing devices, even personal property, such as mobile devices including, but not limited to, cellular phones, personal digital assistants (PDAs), as well as computers.

All such persons as listed above are referred to as "end-users" or "users" within this document.

The term "diocesan" as used herein refers to any and all of the entities named immediately above, as may properly be understood in context.

### **RESPONSIBILITIES**

By using the Diocese of Harrisburg's information technology resources, each end-user accepts the responsibility for his/her behavior and all activities on his/her user identification (ID) and agrees to the following:

- To access only files and data that he/she has created, that are publicly available, or to which he/she has been given authorized access;
- Not to create, access, print, copy, or disseminate documents or content which are contrary to the moral or doctrinal teachings of the Catholic Church for a purpose other than the fulfillment of job-related responsibilities and tasks including, but not limited to, jokes, stories, web site links or pages, and images;
- To use only legal versions of copyrighted software in compliance with vendor license requirements, and not to make or use illegal copies of copyrighted software, store such copies on Diocese of Harrisburg systems, or transmit them over Diocese of Harrisburg networks;
- To be considerate in his/her use of computer system resources and to refrain from overloading networks with excessive data, excessive connect time, disk space, or other resources;

**DIOCESE OF HARRISBURG  
END-USER COMPUTING POLICY**

- Not to use computer programs or other means to decode passwords or access control information;
- Not to engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files;
- Not to use mail or message services intending to harass or intimidate another person;
- Not to disclose his/her password or use another person's password except when required in situations deemed necessary by the Office of Information Technology or, in extenuating circumstances, the person's supervisor;
- Not to use the Diocesan System for personal gain or retribution, for example, by selling access to his/her user ID or password, selling or disclosing organizational data to any unauthorized third party, or by performing work for profit in a manner not authorized by the Diocese of Harrisburg;
- Not to install or operate unauthorized software on diocesan-owned machines;
- Not to violate any statute or regulation of the Commonwealth of Pennsylvania or any of its agencies applicable to the Diocese of Harrisburg and its employees or parishes within the Diocese of Harrisburg and their employees;
- Not to attempt (or assist in an attempt) to:
  - a) Penetrate system security;
  - b) Cause any part of the system to become impaired or inoperable;
  - c) Gain unauthorized access or entry to computer facilities and/or computer based-data;
- Not to copy unauthorized, copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Diocese of Harrisburg or the end user's employer does not have an active license.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

### ENFORCEMENT AND PENALTIES FOR VIOLATIONS

End users should not have an expectation of privacy with regard to their files, data, or communications, whether created on diocesan-owned equipment or personal equipment that accesses diocesan information systems.

The Diocese of Harrisburg considers any violation of this Policy to be a serious offense. The end-user's employer or supervisor reserves the right, at any time and without advance notice, to access, examine, intercept, monitor, and copy the files and/or actual workstation sessions of any user or to suspend a user's access to the system in connection with the investigation including, but not limited to, any of the following:

- Violations or suspected violations of security and/or policies;
- Workstation interactions which may be contributing to poor computer performance;
- Computer malfunctions;
- To maintain the Diocese of Harrisburg's systems;
- Any other purpose deemed appropriate by the Diocese of Harrisburg.

The appropriate employer or supervisor (as well as appropriate Commonwealth agencies and criminal enforcement agencies) may be notified of any violation and provided with information and materials relating to the investigation and/or violation. However, protection of certain files, data, or communications termed "restricted" or otherwise protected by civil or Canon Law, enjoy a great deal of protection and can only be viewed with the express permission of the appropriate diocesan authority.

The responses for violation of this Policy may include, but not necessarily be limited to, any of the following at the sole discretion of the Diocese of Harrisburg:

- Notification: alerting a user to what appears to be an inadvertent violation of this Policy in order to educate the user to avoid subsequent violations.
- Warning: alerting a user to the violation, with the understanding that any additional violation will result in a greater penalty.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

- Loss of computer privileges: limitation or removal of computer privileges, either permanently or for a specified period of time.
- Restitution for damages: requiring reimbursement for the costs of repairs to or replacement of computer-related material, equipment, hardware, software, data and/or facilities, which reimbursement shall include, but not necessarily be limited to, the cost of additional time spent by Diocese of Harrisburg employees or subcontractors due to the violation.
- Disciplinary action: violators may, even for a single transgression, be subject to disciplinary action, up to and including suspension or termination of employment.
- Appeals: If the user wishes to contest the judgment that he/she has violated this Policy or the response made to his/her violation, either the user or the supervisor may make a written request to the Diocesan Office of Mediation Services to assist in resolving the conflict within ten working days of the action.

Furthermore, the violator may be subject to civil or criminal suit pursuant to applicable local, state, and federal ordinances, laws, statutes, or regulations. The violator may also be subject to discipline in accordance with applicable provisions of the Canon Law of the Catholic Church.

### ACQUISITION

The Diocese of Harrisburg will make every effort to meet the technological needs of the diocese by purchasing appropriate computer hardware and software. The Office of Information Technology will be responsible for setting technology standards and minimum standards for connectivity to the Diocesan Network as appropriate.

The Office of Information Technology must review all potential hardware and software acquisitions either by purchase or donation, including any mobile access devices (including, but not limited to, cellular phones and PDAs), prior to purchase by diocesan personnel or subcontractors in order to ensure compatibility for successful installation, implementation, and support. This includes the

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

acquisition of all Catholic Charities, parish, or school computers and related hardware and software that will be connected to the Diocesan Network.

### **INFORMATION SECURITY**

The Office of Information Technology is responsible for establishing and maintaining the physical security of the central computing facilities, the Diocese of Harrisburg's communications network, and data for which the Office of Information Technology is the custodian.

### **ACCESS CONTROL**

The Diocese of Harrisburg provides access to computing resources for the exclusive use of diocesan, parish, school, and Catholic Charities personnel, and for the purposes of advancing religious and institutional pursuits and certain administrative support functions. The Office of Information Technology is responsible for instituting and monitoring appropriate access control measures for centrally managed computer systems including file servers and other systems for which it has system administration responsibilities. Access to central computing systems is granted by the issuance of an individual user logon identification, password protection, and usage restrictions as appropriate. In addition to these general access controls, compliance with procedures for granting access to particular software applications or data is also required. The Office of Information Technology must receive appropriate end-user data access approvals from the appropriate employer, supervisor or, where applicable, the application data owner.

Individual users assume responsibility for the appropriate and ethical use of the systems and data to which they have access. Misuse of Diocese of Harrisburg computers, communication devices, data, or other information technology resources is a serious offense. Violators are subject to disciplinary and/or legal action. Misuses of information technology resources include, but are not limited to, improperly using Diocese of Harrisburg data, computer equipment, or proprietary software, accessing Diocese of

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

Harrisburg computers with stolen or illegitimate user identification, and compromising the security or performance of shared computer or communication systems. End-users are expressly prohibited from installing or operating unauthorized software on diocesan-owned machines.

### **DIOCESAN NETWORK ACCESS**

The Office of Information Technology provides access to information, systems, and services at other diocesan sites, Catholic Charities, and parish or related sites (e.g. inter-parochial schools) within the Diocese of Harrisburg by providing inter-network connectivity to the Diocesan Network. Requests for new users, user modifications, or deletion of user accounts or access rights, must be submitted to the Office of Information Technology at least five (5) business days in advance of the effective date. The Office of Information Technology should be notified immediately of any unscheduled employee terminations.

At least one computer in each diocesan, Catholic Charities, parish, and school site must be connected to the Diocesan Network. To ensure this connectivity, it is the responsibility of each site to comply with certain minimum computer requirements as determined by the Office of Information Technology. This includes access to the Internet through an Internet Service Provider. Changes and additions to computers and associated peripherals accessing the Diocesan Network must be scheduled at least five (5) business days in advance and coordinated with the Office of Information Technology. Requests not received within the five day time frame will be processed as the Office of Information Technology workload permits.

Requests by diocesan employees for computer-related assistance must come through the Diocesan Help Desk System at [www.help.hbgdiocese.org](http://www.help.hbgdiocese.org) or by sending an email to [helpdeskmail@hbgdiocese.org](mailto:helpdeskmail@hbgdiocese.org). Requests for assistance via telephone calls and emails to specific Office of Information Technology staff will not be given priority. The emergency hotline Help Desk extension (281) is available and is to be used for emergency purposes. Emergencies constitute a stoppage of work.

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

### **BACKUP/RECOVERY**

The Office of Information Technology is responsible for maintaining an appropriate back-up schedule and rotation for all critical data. Any data not stored on the central Diocesan Network servers located in the Diocesan Center is the sole responsibility of the owner for back-up and recovery. It is the responsibility of the parish, school, or Catholic Charities to understand where files are stored and how they are backed up.

The Office of Information Technology will maintain a disaster recovery procedure for all diocesan-level applications and network resources and are responsible for testing and documentation. Parish, school, and Catholic Charities sites are responsible for site-level applications, data, and recovery procedures.

### **SYSTEMS DEVELOPMENT AND MAINTENANCE**

The Office of Information Technology provides systems analysis and application support services that maintain the Diocese of Harrisburg's administrative functionality. These services include the design, implementation, support, documentation, testing, and maintenance or enhancement of computer systems for financial accounting, integrated record-keeping, payroll processing, document imaging, web site content management, etc. as requested by Diocese of Harrisburg departments, under direction of the Secretariat for Administrative Services.

### **PASSWORD MANAGEMENT**

#### **General**

Password management is the selection, distribution, use, and modification of computer system passwords. Effective password management is the most central single element in assuring the overall security of the Diocese of Harrisburg's information systems and the protection of its information assets.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

### **Responsibilities**

All participants in the use and administration of the Diocese of Harrisburg's technology resources share responsibility for effective password management. Specific responsibilities are assigned as follows:

- The Office of Information Technology shall independently establish minimum baseline standards for passwords on all multi-user systems for which it has responsibility. These standards shall include minimum length, characteristics, and expiration cycles.
- Software systems or particular applications may require access passwords beyond those required for accessing the computer system itself. The owner of the software application system, or, where applicable, the application data owner, establishes requirements for such passwords.
- End-users are responsible for the security of individual computing equipment and information stored on local disk drives. In addition, end users are responsible for the content of any removable media (such as USB drives, diskettes, and CD's or DVD's) that contain diocesan information in accordance with the Remote Access and Removable Media Policies.
- Ultimately, users of the Diocese of Harrisburg's computer systems are responsible for assuring effective password management. To fulfill this responsibility, they shall be aware of and follow the password management standards for each system they access. Most notably, this includes choosing strong passwords and safeguarding their integrity. Computer passwords represent an individual's identity to the system and should never be disclosed to or used by others except when required in situations deemed necessary by the Office of Information Technology or, in extenuating circumstances, the person's supervisor.
- Unauthorized use of a computer ID is a violation of Diocese of Harrisburg Policy, and violators may be subject to disciplinary action, including suspension or termination of employment.

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

### **REMOVABLE MEDIA**

Removable media is a well-known source of malware infections and has been directly tied to the loss of sensitive information in many organizations. Removable media is defined as a device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer. This includes flash memory devices such as thumb drives, cameras, MP3 players, and PDAs; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks, and any commercial music and software disks not provided by the Diocese of Harrisburg.

In order to minimize the risk of loss or exposure of sensitive information maintained by the Diocese of Harrisburg and to reduce the risk of acquiring malware infections on computers operated by the Diocese of Harrisburg, users may only use removable media in their work computers. Removable media may not be connected to, or used in, computers that are not owned or leased by the Diocese of Harrisburg without the explicit prior written permission of an employee of the Office of Information Technology. Sensitive information should be stored on removable media only when required in the performance of assigned duties, and the data should be encrypted whenever possible.

Any user found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

### **MOBILE DEVICES**

Use of mobile devices, including, but not limited to, laptop computers, personal digital devices (PDAs), and cellular phones, whether diocesan or personal property, must be used only for business purposes and in a manner consistent with these Policies if they connect to or access the Diocesan Network and/or are used during working hours. Employees using mobile devices as part of their job duties must do so in a safe manner and are prohibited from using mobile devices while operating a vehicle.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

### REMOTE ACCESS

The purpose of this Policy is to define standards for connecting to the Diocesan Network from any computer or access device. These standards are designed to minimize the potential exposure to the Diocese of Harrisburg from damages which may result from unauthorized use of its resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical diocesan internal systems, etc.

- This Policy applies to all users with a diocesan-owned or personally-owned computer or workstation used to connect to the Diocesan Network. This Policy applies to remote access connections used to do work on behalf of the Diocese of Harrisburg, including reading or sending email and viewing intranet or Internet web resources.
- Remote access implementations that are covered by this Policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.
- It is the responsibility of the user with remote access privileges to the Diocesan Network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
- Secure remote access must be strictly controlled. Control will be enforced via authentication or public/private keys with strong passwords.
- At no time should any user provide their login or email password to anyone, even family members or co-workers, except when required in situations deemed necessary by the Office of Information Technology or, in extenuating circumstances, the person's supervisor.
- Diocesan users with remote access privileges must ensure that their diocesan-owned or personal computer or workstation, which is remotely connected to the Diocesan 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. The computer must be up-to-date with the most recent anti-virus signature files and Microsoft Windows updates.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

- Any user found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment, as well as potential civil liability.

### **ELECTRONIC MESSAGING**

#### **Introduction**

A variety of electronic communication mechanisms are available to individuals and groups at the Diocese of Harrisburg. These *electronic messaging systems* are an alternative to paper-based letters, memos, posters, fliers, and bulletin board notices. They currently include such systems as electronic mail, public folders and forms, instant messaging, and the World-Wide Web. Electronic messaging systems of the Diocese of Harrisburg provide a medium for information exchange and are provided to support its services, communications, and administrative activities. This Policy sets forth responsibilities and principles that shall direct the use of the Diocese of Harrisburg's electronic messaging systems, both internally and in conjunction with the global electronic community.

#### **Responsibilities**

All end-users are encouraged to use electronic messaging resources and are expected to do so in a manner consistent with the Diocese of Harrisburg's mission. Use of the messaging systems commits individuals to all applicable Diocese of Harrisburg policies, procedures, and regulations. Local, state, and federal laws may apply as well, as may the Canon Law of the Catholic Church.

Users shall obey applicable laws and regulations regarding data use and information security. Since electronic messaging systems may carry information in the form of personal and/or casual communication as well as official Diocese of Harrisburg data, care must be taken to ensure that the two are clearly distinguished.

The Office of Information Technology is responsible for ensuring reliable, secure, and efficient operation of the Diocese of Harrisburg's electronic messaging systems. The Office of Information

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

Technology shall also assure access to messaging services for all end-users in keeping with the mission of the Diocese of Harrisburg.

### **Principles**

While privacy cannot be assured on all systems in a particular message route, the Office of Information Technology will work to assure system security and availability on the computer systems it administers. Recipients of electronic messages must also be aware that the identity of the sender may or may not be authentic. Even though the identity of the message sender is not authenticated by many of the current messaging systems, forgeries are nonetheless unacceptable. Also, senders must be aware that delivery of a message cannot be fully assured. As with paper mail, response from the recipient is the only reliable way to determine that a message has been received and read. Messages from unknown sources should not be opened; likewise electronic mail attachments should not be opened unless the recipient is fully familiar with its sender and contents.

### Transportation Versus Storage

Because there is a limited amount of storage space for new/incoming messages contained in the messaging systems, it is not to be used for long-term storage or archive. Instead, electronic messaging systems are to be considered a transportation mechanism. As with any transportation mechanism, the related issues of system failure and recovery should be considered. While the Office of Information Technology will perform periodic backups of messages in transit, these should be viewed as insurance against system failure, not as a mechanism to restore individual messages. Size limits will be imposed on all electronic mail accounts. Exceeding the limits may result in the inability to send or receive electronic messages. Electronic mail folders should be cleaned and items deleted on a regular basis, at least monthly. Electronic mail that involves records subject to the Diocese of Harrisburg's Records Retention Policy should be preserved in accordance with that Policy.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

### Global Connectivity

Connection to global networks such as the Internet and use of World Wide Web services pose additional challenges. Each network, mailing list, and news group has its own policies, procedures, and rules of conduct.

### Cost

The costs associated with electronic messages are unlike those for traditional paper-based mail. The cost of electronic messages is born primarily by the recipient(s), not the sender. **Therefore, no junk mail shall be sent using Diocese of Harrisburg messaging systems.** Specific examples of junk mail are: chain letters, advertisements, and other unsolicited mass mailings, as well as excessive or inappropriate (as determined by the user's employer or supervisor) postings to news groups, distribution lists, or public folders.

### Message Content

The content of any message sent through the messaging system is the sole responsibility of the individual sending the message. Harassment, obscenity, forgery, pornography, and other illegal forms of expression are not acceptable use of Diocese of Harrisburg resources. The only enforceable restrictions on content of electronic messages are those that apply generally to verbal or written communication (slander, harassment, etc.). When such restrictions need to be enforced, the same administrative, judicial, and criminal processes as for non-computer communication may be invoked; use of electronic messaging systems does not change what is and is not an illegal communication.

In an effort to protect its computing resources, the Diocese of Harrisburg reserves the right to use content filtering software to block any electronic mail from/to any sender/recipient. The content filtering software is intended to block delivery of junk email, advertisements, sexually explicit, and pornographic messages. Blocking can be based upon subject line, sender, domain, or key words in the message body. It is possible that valid messages could be blocked. If a user

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

suspects that a valid email has been blocked, he/she can contact the Office of Information Technology through the Help Desk for verification and resolution.

The Diocese of Harrisburg will not censor or regulate messages based on views expressed by the sender or implied by the receipt. Transmission of information by electronic means does not negate intellectual property rights, copyrights, or other protections.

Neither the Diocese of Harrisburg, nor any parish, Catholic institution, nor Catholic school within the Diocese of Harrisburg, accepts any responsibility for damages or offenses caused by individuals who use the messaging systems of the Diocese of Harrisburg for any purpose or in any manner contrary to this Policy.

Instant messaging (IM) is a form of email or text communication and, like all other forms of email, it creates a written business record that can be subpoenaed and used as evidence in litigation or regulatory investigations and may need to be preserved as part of a litigation hold as described in the Diocese of Harrisburg's Records Retention Policy.

Like all other electronic communications, the Diocese of Harrisburg has the right to access and review the content of any electronic or text message, including IM, that is created, stored, transmitted, or received using resources provided by the diocese, including those sent and received via personal IM tools on public networks.

The following actions are considered a violation of acceptable email conduct:

- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages;
- Unauthorized use or forging of email header information;
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type;

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

- Use of unsolicited electronic messages originating from within the Diocese of Harrisburg's networks, or from any service hosted by the Diocese of Harrisburg or connected via the Diocese of Harrisburg's network;
- Posting the same or similar non-business-related messages to distribution groups or large numbers of Usenet newsgroups (newsgroup spam).

### **Enforcement**

Electronic messaging systems by their very nature depend on the shared effort and responsibility of all who participate in and manage their use. Disruptions, whether by technical or behavioral means, can impact availability and usefulness for an entire community of users. The Diocese of Harrisburg reserves the right to manage its electronic messaging resources (medium and services) to ensure overall utility and common accessibility in support of the mission of the Diocese of Harrisburg.

### **INTERNET USAGE AND SECURITY**

The Diocese of Harrisburg provides access to the vast information resources of the Internet as a business tool for end-users. The facilities to provide that access represent a considerable commitment of diocesan resources for telecommunications, networking, software, storage, etc. This Internet Usage Policy is designed to help end-users understand the Diocese of Harrisburg's expectations for the use of those resources in the particular conditions of the Internet and to help them use those resources wisely.

End-users accessing the Internet are to conduct themselves honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy, and prerogatives of others just as they would in any other business dealing. To be absolutely clear on this point, all existing diocesan Policies apply to end-users' conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of diocesan resources, sexual harassment, information and data security, and confidentiality.

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the Diocese of Harrisburg and expose the diocese to significant legal liabilities.

The chats, newsgroups, and email of the Internet give each individual Internet user an immense and unprecedented reach to propagate diocesan messages. Because of that power, special care must be taken in order to maintain the clarity, consistency, and integrity of the Diocese of Harrisburg's image and posture. Anything a user writes in the course of acting for the Diocese of Harrisburg on the Internet can be taken as representing its organizational posture.

While the Diocese of Harrisburg's direct connection to the Internet offers a wealth of potential benefits, it can also open the door to some significant risks to data and systems if appropriate security discipline is not followed. Security is to be everyone's first concern. An Internet user can be held accountable for any breaches of security or confidentiality.

### **Detailed Internet Policy Provisions**

- The Diocese of Harrisburg has software and systems in place that can monitor and record all Internet usage. Each Internet user should be aware that these security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, and each file transfer into and out of the Diocesan Network. No end-user should have any expectation of privacy as to his or her Internet usage. The Office of Information Technology will review Internet activity and analyze usage patterns to ensure that Internet resources are devoted to maintaining the highest levels of productivity.
- The Diocese of Harrisburg reserves the right to inspect any and all files stored in private areas of its network in order to assure compliance with Policy.

## DIOCESE OF HARRISBURG END-USER COMPUTING POLICY

- The display of any kind of sexually explicit image or document on any diocesan system is a violation of its Policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using the Diocesan Network or diocesan computing resources.
- The Diocese of Harrisburg uses independently-supplied software and data to identify inappropriate or sexually-explicit Internet sites and reserves the right to block access to any Internet web site.
- The Diocesan Network's Internet facilities and computing resources must not be used knowingly to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province, Canon Law, or other local jurisdiction in any material way. Use of any diocesan resources for illegal activity is grounds for immediate dismissal; the Diocese of Harrisburg will cooperate with any legitimate law enforcement activity.
- Any software or files downloaded via the Internet into the Diocesan Network become the property of the Diocese of Harrisburg. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
- No end-user may use diocesan facilities knowingly to download or distribute pirated software or data.
- No end-user may use the diocesan Internet facilities to deliberately propagate any virus, worm, Trojan horse, or trap-door program code.
- No end-user may use the diocesan Internet facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- Each end-user using the Internet facilities of the Diocese of Harrisburg shall identify himself or herself honestly, accurately, and completely (including one's diocesan affiliation and function

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

- Use of diocesan Internet access facilities to commit infractions such as misuse of diocesan assets or resources, sexual harassment, unauthorized public speaking, and misappropriation or theft of intellectual property are also prohibited.
- Video and audio streaming and downloading technologies represent significant data traffic which can cause local network congestion. Video and audio downloading should be scheduled for off-peak times.
- The Diocese of Harrisburg has installed firewalls and other security systems to assure the safety and security of its networks. Any end-user who attempts to disable, defeat, or circumvent any security facility will be subject to immediate dismissal.

### **POLICY ON POSTING OF INFORMATION ON THE INTERNET**

The Internet is a public forum with unrestricted access. For this reason, the Diocese of Harrisburg, including its parishes, Catholic Charities, and schools, restricts the posting of information related to the Diocese of Harrisburg, its parishes, Catholic Charities, schools, employees, and students on the Internet. No person is permitted to use images of the Diocese of Harrisburg, parishes, Catholic Charities, schools, any diocesan-related logos or seals, school or diocesan staff, or students in any form on the Internet or in any form of electronic communication, including a chat room, e-mail, social network, or other messaging system without the prior written permission from diocesan or school administration or the Information Technology Director of the Diocese of Harrisburg.

Further, the posting or transmission of images or information in any format related to the Diocese of Harrisburg, its parishes, Catholic Charities, schools, employees, and students that are defamatory, scurrilous, pornographic, or which could be construed as threatening or impugning the character of another person, is similarly prohibited and will subject the person(s) involved in the posting or

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

transmission of such material to disciplinary action deemed appropriate by the administration at the parish, school, Catholic Charities, and/or by the Diocese of Harrisburg, and legal action will be taken where appropriate.

### **BLOGGING**

- Blogging by employees, whether using Diocese of Harrisburg's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Blogging entries are subject to monitoring.
- Employees are prohibited from revealing any Diocese of Harrisburg confidential, proprietary information, or trade secrets when engaged in blogging.
- Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the Diocese of Harrisburg and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory, profane, or harassing comments when blogging or using any other electronic access device.
- Employees may also not attribute personal statements, opinions, or beliefs to the Diocese of Harrisburg when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the Diocese of Harrisburg.
- Employees assume any and all risk associated with blogging. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Diocese of Harrisburg logos or any other Diocese of Harrisburg intellectual property may also not be used in connection with any blogging activity.

### **DIOCESAN WEB SITE**

Each Diocesan Secretary is responsible for the content and updating of information contained in their respective sections of the diocesan web site. New pages, sections, and any content to be added to

## **DIOCESE OF HARRISBURG END-USER COMPUTING POLICY**

the web home page must first be approved by the Director of the Office for Communications under the direction of Office of the Vicar General. Parishes, schools, and other Catholic institutions within the Diocese of Harrisburg having their own web sites may be linked from the main diocesan web site. The Office of Information Technology will be responsible for maintaining the web hosting file server, web infrastructure, and database structure.

### **VIRUS PROTECTION**

All file servers and computers in the Diocesan Center are protected by anti-virus software that is constantly updated. Any computer that is connected to the Diocesan Network must have virus protection software licensed, installed, operational, and actively updated. Updates to anti-virus signature files are automated for Diocesan Center workstations. As new viruses become a threat, the Office of Information Technology will check with the appropriate authorities and communicate valid virus information to members of the Diocesan Network when necessary.

**DIOCESE OF HARRISBURG  
END-USER COMPUTING POLICY**

"I have received and read a copy of the Diocese of Harrisburg's End-User Computing Policy. I fully understand and accept the terms of this Policy and agree to abide by it. I also understand that this Policy can be changed or updated at any time, and that I would be informed of such changes. I acknowledge and understand that any violation of this Policy could lead to dismissal or even criminal prosecution as warranted. I also acknowledge and understand that any damages as a result of my actions in not adhering to this Policy could be withheld from my pay."

\_\_\_\_\_  
End-User Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Name (printed)

\_\_\_\_\_  
Office/Location Name (printed)

\_\_\_\_\_  
Location City (printed)

Affiliation (check one):  Employee     Contractor/Vendor/Consultant     Volunteer

This Policy is hereby promulgated within the Diocese of Harrisburg by the Bishop of Harrisburg, the Most Reverend Kevin C. Rhoades, and such Policy becomes effective immediately. All prior provisions of Diocesan Statute or Policy are hereby abrogated. This Policy is to be disseminated in a manner determined by the Office of Information Technology of the Diocese of Harrisburg.

Given in Harrisburg, Pennsylvania, this 1st Day of April, 2009.

*+ Kevin C. Rhoades*  
Most Reverend Kevin C. Rhoades  
Bishop of Harrisburg

In witness whereof I affix my signature...

*Carol L. Houghton*  
Carol L. Houghton, STD, JED  
Chancellor

**DIOCESE OF HARRISBURG  
END-USER COMPUTING POLICY**

**Appendix A**

**GLOSSARY**

**Anti-virus Signature Files** – Signature based detection is the most common method that antivirus software uses to identify malicious software. This method is somewhat limited by the fact that it can only identify known viruses, unlike other methods. When antivirus software scans a file for viruses, it checks the contents of a file against a dictionary of virus signatures. A virus signature is the viral code. So, saying you found a virus signature in a file is the same as saying you found the virus itself. If a virus signature is found in a file, the antivirus software can take action to remove the virus.

**Blogging** - A blog (a contraction of the term "Web log") is a Web site, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order. "Blog" can also be used as a verb, meaning to maintain or add content to a blog. Many blogs provide commentary or news on a particular subject; others function as more personal online diaries. A typical blog combines text, images, and links to other blogs, web pages, and other media related to its topic. The ability for readers to leave comments in an interactive format is an important part of many blogs.

**DSL** – DSL is a family of technologies that provides digital data transmission over the wires of a local telephone network. DSL originally stood for digital subscriber loop, although in recent years, the term digital subscriber line has been widely adopted as a more marketing-friendly term for ADSL, which is the most popular version of consumer-ready DSL. DSL can be used at the same time and on the same telephone line with regular telephone, as it uses high frequency, while regular telephone uses low frequency.

**Frame Relay** – Frame Relay consists of an efficient data transmission technique used to send digital information. It is a message forwarding "relay race" like system in which data packets, called frames, are passed from one or many start-points to one or many destinations via a series of intermediate node points.

**ISDN** - Integrated Services Digital Network is a telephone system network. Prior to the ISDN, the phone system was viewed as a way to transport voice, with some special services available for data. The key feature of the ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system.

**Malware** – Short for malicious software, malware is software designed to infiltrate or damage a computer system without the owner's informed consent. The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software.

**PDA** - Short for personal digital assistant, a PDA is a handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer.

**DIOCESE OF HARRISBURG  
END-USER COMPUTING POLICY**

**Appendix A**

**GLOSSARY - Continued**

**Strong Password** - A strong password is one which is difficult to guess by other humans or by password hacking tools. A strong password complies with criteria which are proven to be more difficult to guess or hack. It includes the use of a minimum number of characters, the use of multiple characters (upper/lower case, numeric and special characters) and the prevention of reusing passwords within a given timeframe.

**VPN** - A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.