Roman Catholic DIOCESE OF ROCKVILLE CENTRE

Policy and Procedure Guidelines for Technology

Prepared by the Office of Information Technology

January 2014

INTRODUCTION

The Computer, E-Mail and Internet Usage Policy (the "Guidelines") is the compilation of policies concerning the technology implemented and relied upon by the Roman Catholic Diocese of Rockville Centre (the "Diocese") in the fulfillment of its mission. The Guidelines have been formally adopted by the Diocese and form a part of the current Human Resources policies of the Diocese. In addition, the Guidelines apply to all persons who enter or come in contact with the Diocese's many locations or technology. Persons covered by these policies include all lay employees, religious and clergy who work for or with the Diocese, as well as all independent contractors, vendors or other individuals who may have reason and permission to access the technology platforms maintained by the Diocese. All questions concerning the interpretation or application of these Guidelines should be directed either to your manager, the Office of Information Technology or the Office of Human Resources. Violation of any of the policies contained in the Guidelines, may result in immediate employment action, including, but not limited to, termination of employment.

General Acceptable Use Policy Statement

Internet-, Intranet- Extranet-related systems and stand alone workstations provided by the Diocese, including, but not limited to, computer equipment, communication devices, software, operating systems, storage media, network and email accounts , web browsing, and file transfer protocol utilities, are the property of the Diocese. These systems are to be used ONLY for business purposes in serving the interests of the Diocese. No person is expressly, implicitly or otherwise authorized to use the property of the Diocese for personal use or outside of the scope of these Guidelines.

Effective computer security is a team effort involving the participation and support of every individual who provides services to, or on behalf of, the Diocese and who deals with its information and/or information systems. Thus, it is the responsibility of every computer user to be familiar with the Guidelines, and to conduct their activities accordingly.

Purpose

The purpose of the Guidelines is to outline the acceptable usage of computer equipment and practices at the Diocese. The Guidelines are in place to protect the individual user and the Diocese. Inappropriate use of and related technologies exposes the Diocese to several risks, including virus & spyware attacks, the compromising of network systems which can cause system outages and unforeseen liabilities.

The Diocese provides its employees with computer systems to facilitate business communications and to enhance productivity. As with the telephone, there may be occasion to use the computer systems for personal purposes. Personal use is permitted so long as such use conforms to these Guidelines and does not interfere with job performance, consume significant resources or interfere with the activities of other employees.

Under no circumstances shall the computer systems be used for personal financial gain or to solicit others for activities unrelated to the Diocese business or in connection with political campaigns or lobbying.

Scope

The Guidelines apply to clergy, religious, lay employees, contractors, consultants, temporary employees, interns, volunteers and all other individuals providing services to or on behalf of the Diocese, including all personnel affiliated with third parties. The Guidelines also apply to all information-technology-related equipment, databases or applications, and websites that are owned or leased by the Diocese and hosted on Diocesan equipment or by a vendor.

1. Policy Statement

General Use and Ownership –

While the Diocese seeks to provide a reasonable level of privacy regarding the information contained or otherwise stored on the systems maintained by offices of the Diocese, individual users should be aware that the data they create or save on these systems remains the property of the Diocese. Accordingly, no individual

should have any expectation of privacy as respects to the content or data contained in his or her computer or their network drives. For security and network maintenance purposes, authorized individuals within the Office of Information Technology may monitor equipment, systems and network traffic at any time, in accordance with standard industry operating procedures. The Office of Information Technology has been charged with the role of auditing networks and systems on a periodic basis to ensure compliance with the Guidelines.

2. Unacceptable Use Policy

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

a. Under no circumstances is an individual user authorized or permitted to engage in any activity that is considered illegal under church, local, state, federal or international law while utilizing Diocesan-owned resources. The following are among those activities that are strictly prohibited: (1) downloading of material such as 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) installation of any unlicensed software for which the Diocese does not have an active license. (4) Transmission of any material in violation of any church, local, state, federal or international law or regulation is also strictly prohibited. (5) Use of software files, images or other information downloaded from the internet that has not been released for free publication.

b. The following activities are strictly prohibited: transmission or downloading of content that violates copyrights held by others; transmission of threatening, violent, or obscene material; and transmissions that contain inappropriate language and communications.

c. Acts of vandalism are prohibited. Vandalism is defined as any malicious attempt to harm or destroy data of another user or to damage hardware or software. This includes, but is not limited to, the uploading or creation of computer viruses or stealing of personal information for identity theft purposes.

d. Unauthorized use of another individual's computer, access accounts, and/or files is prohibited.

e. The following System and Network activities are strictly prohibited, without exception:

• Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

• Revealing an account password to others or allowing use of one's account by others, including interns, volunteers and contractors.

• Using a Diocesan computer or technology information resource to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws or for personal financial gain.

• Engaging in any conduct that violates policies of the Diocese.

- Using the technology resources of the Diocese to engage in such conduct as making fraudulent offers of products, items, services or support of personal business.

- Entering into contractual agreements via the Internet (e.g., into a binding contract on behalf of the Diocese over the Internet)

- Using Diocese resources to impersonate someone else.

f. The following E-mail and Communications activities are strictly prohibited, without exception:

• Sending 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 in-person, e-mail, telephone or paging, whether through language, frequency, or size of messages.

• Unauthorized use, or forging, of e-mail header information or digital signatures.

• 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.

• Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

• Use of unsolicited e-mail, originating from within the Diocesan networks, of other Internet, Intranet or Extranet service providers.

• Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam).

• Use of the Diocesan logos or materials in any web page or Internet posting or printed material, unless it has been approved in advance by the Diocesan management.

3. Audit Policy

The Diocese has adopted a technology Audit Policy, the overall purpose and application of which are as follows:

a. Purpose - to enable the Diocese to maintain its systems and to monitor the use of the systems consistent with the acceptable use terms of the Guidelines.

b. Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources.
- Investigate possible security incidents to ensure conformance to Diocesan security policies.
- Monitor user or system activity where appropriate.
- Monitor and record Internet, Network, and E-mail activity.

c. Audits conducted by:

- Outside vendors such as KPMG or the IT support company.
- Internal members of the Office of Technology

Scope

The Audit Policy covers all computer and communication devices owned or operated by the Diocese, as well as any computer and communication devices that are present or connected to the equipment or technology resources maintained by or on Diocesan premises, but which may not necessarily be owned or operated by the Diocese.

Policy

When requested, and for the purpose of performing an audit, any access needed will be provided to members of the Office of Information Technology team or any authorized user acting on behalf of the Office of Information Technology.

This access may include:

- User level and/or system level access (administrator privileges) to any computing or communications device.
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Diocesan equipment or premises.
- Access to work areas (offices, cubicles, storage areas, etc.).

4. Automatically Forwarded E-mail Policy

The Diocese has adopted a policy of prohibiting automatically forwarded E-mails to the personal accounts of the employees of the Pastoral Center, unless approved by the Office of Information Technology or Senior Management. The overall purpose of which is to prevent the unauthorized or inadvertent disclosure of sensitive company information.

Scope

This policy covers all automatic e-mail forwarding, and seeks to prevent the potentially inadvertent transmission of sensitive information by employees, vendors, and agents operating on behalf of the Diocese.

Policy

Employees must exercise utmost caution when sending any e-mail from inside the Diocese to an outside network. Unless pre-approved by the Office of Information Technology, no Diocesan e-mail may be automatically forwarded to an external destination for any employee of the Pastoral Center.

5. Computer Password Policy

Passwords are a critical aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Diocese's entire corporate network. As such, all authorized individual users (including, but not limited to, outside contractors and vendors who may need to be granted access to the Diocese's technology resources for the purpose of supporting a particular of operations) of Diocesan technology resources, platforms and networks are responsible for taking all appropriate steps, as outlined below, to secure their passwords.

Purpose

The purpose of the Password Policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change of passwords. The Diocese has implemented a mandatory policy within its Active Directory structure that applies these standards to all computer workstations and laptops that reside within this domain.

Scope

The Password Policy applies to all individual authorized users who (i) have or are responsible for an account (or

any form of access that supports or requires a password) on any system that resides at any Diocesan facility; (ii) have access to the Diocesan network; or (iii) store any non-public Diocesan information via Diocesan technology.

Policy

The Password Policy is comprised of the following elements:

- All user-level passwords will be changed every 90 days.
- Each user will be responsible for creating their own password.
- All passwords must be at least 8 characters long and contain a combination of the following:

    - They will contain upper and/or lower case characters (e.g., a-z, A-Z)
    - The will consist of numbers, punctuation characters and letters (e.g., 0-9, !,@,#,$,%,^,&,*,(,),_,+,|,~,-,=,\,`,{,},[,],:,",;,',<,>,?,,,.,/).

PASSWORDS MUST NOT BE SHARED. All passwords must be treated as sensitive and confidential Diocesan proprietary information.

6. Anti-Virus Software and Process

All computers systems of the Diocese are protected by our enterprise anti-virus software application. Any outside computer that needs to attach to the Diocese internal network will be reviewed to ensure that the device has anti-virus software installed and has the latest anti-virus update. The following are general practices whereby, through simple preventative measures, all Diocesan personnel can take steps toward the protection of Diocesan Technology Resources:

a. NEVER open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. These files may contain viruses, e-mail bombs, or Trojan horse code.
b. Delete attachments to e-mails that are from an unknown, suspicious or untrustworthy sources immediately, then "double delete" them by emptying your Recycle Bin/Trash.
c. Delete spam, chain, and other junk e-mail without forwarding.
d. Never download files from unknown or suspicious sources.
e. Always scan a floppy diskette or any portable media from an unknown source for viruses before using it.
f. If you receive an e-mail warning you about a virus, contact the Office of Information Technology immediately. DO NOT send it to other employees or contacts outside the Diocese.

7. File Management

The following are the standard guidelines for the maintenance of data files on the Diocese's Technology Resources:

a. The primary location for storing all Diocesan files is on the Diocesan network.
b. Users are responsible for management of network directories under their purview.
c. Each user shall review the contents of his/her home/personal directory at least once every six months to remove extraneous material. Same applies for all department shares.
d. All users should never save data to the local hard drive (better known as the C drive).

8. Equipment Management

The following are the standard guidelines for the use of equipment in connection with the Diocese's Technology Resources:

a. No personal equipment, such as printers, scanners, laptops/Ipads or other equipment is permitted to be connected to the Diocesan network or other Diocesan Technology Resources.
b. Standard equipment configurations should not be changed under any circumstances or by any individual user.
c. All equipment provided to authorized individual users remains the property of the Diocese throughout the equipment's life cycle.
d. Individual users are responsible for safeguarding the equipment/technology resources entrusted to them.
e. All computer equipment and software will be purchased by the Information Technology department.

9. Software Management

The following are standard guidelines for the use of Software in connection with the Technology Resources of the Diocese:

a. Personal software should not be installed on Diocesan equipment.
b. Software should not be downloaded and/or installed from the Internet unless approved by the Office of Information Technology.
c. The Office of Information Technology is responsible for the installing of ALL software.
d. The Office of Information Technology is responsible for maintaining an inventory of all Diocesan computer software installed on all Technology Resources.
e. The Office of Information Technology will periodically evaluate or review the inventory for all hardware and software via on-site inspection and verify that sufficient licenses are on hand to cover all installed applications.
f. All software installs must have a valid license.

10. Training and Orientation

The Office of Information Technology will provide training classes when requested to help individual authorized users achieve a basic familiarity with the standard technology packages used by the Diocese. No advanced training or training in non-standard applications is provided unless instructed by Senior management.

The training offered and provided by the Office of Information Technology grants access to requisite training and/or orientation and establishes the standard guidelines for the ongoing education of individual technology users.

Supervisors are responsible for identifying individual user training needs and working with the Office of Information Technology to meet such needs.

Individual Users are responsible for identifying their own training needs and should bring these needs to the attention of their supervisors.

11. Voicemail

Voicemail boxes may be issued to Diocesan employees who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a password which must never be the same as the default setup password. (See Appendix A – Changing your voicemail password) Voicemail boxes are reviewed once a year (during the summer months) to verify active status.

12. Personal Communication Devices

The Diocese has adopted the following policy regarding the issuance and use of Personal Communication Devices for Diocesan business.

Scope

This policy applies to any Personal Communication Device (commonly known as PDA's or cell or smart phones) issued by the Diocese and used for Diocesan business.

Policy

Personal Communication Devices (PCD) will be issued only to Diocesan personnel whose duties require them to be in immediate and frequent contact when they are away from their normal work locations. Personal Communication Devices are defined to include handheld wireless devices such as Blackberrys, cell or smart phones, wireless laptops, and other similar devices. Blackberry devices are the only PDA supported by the Office of Information Technology. In the event where the Information Department or Senior Management allows access of Corporate email on a personal cell phone, the user must allow the installation of a management agent on his or her personal device.

Loss or Theft

Files containing confidential or sensitive data may not be stored in PCDs unless the device is protected by a password. Lost or stolen equipment must be reported immediately to the Office of Information Technology or the Human Resources department.

PCD Safety

Conducting telephone calls or utilizing PCDs while driving can be a safety hazard. Drivers should use PCDs while parked or out of the vehicle. If employees must use a PCD while driving, the Diocese of Rockville Centre requires the use of hands-free enabling devices as stated by New York State laws.

13. Mobile Computing & Storage Devices

Scope

This policy pertains to all devices connected to the network of Diocese of Rockville Centre. Only authorized devices should be connected unless approved by Diocese management. 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, wireless access points and any other existing or future mobile computing or storage device.

Policy

It is the policy of the Diocese that mobile computing and storage devices containing or accessing information resources at the Diocese must be approved by the Office of Information Technology prior to connecting to Diocesan information systems or network.

Only Diocesan provided flash drives will be permitted on the network. All users who require a flash drive must first have approval emailed from their director to the IT Help Desk. The IT Help Desk will provide a temporary flash drive for use. These flash drives will be collected and scanned periodically for viruses and other malicious content.

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 Diocese.

14. Remote Access

The Diocese has adopted the following Remote Access Policy in order to establish applicable rules regarding

remote access to Diocesan information resources. This policy seeks (i) to protect information when accessing the corporate network via remote access methods and (ii) to safeguard acceptable use of the Diocesan network.

Scope

This policy applies to all Diocesan employees, contractors, vendors, and agents with a Diocese- owned or personally-owned computer or workstation used to connect to the Diocesan network. This policy applies to remote access connections used to work on behalf of the Diocese and includes reading or sending email and viewing intranet web resources.

"Remote access" definition is defined as not being connected directly to the Diocese network but via a third party medium such as "GOTOMYPC" application or similar ones or a VPN connection.

There are limited resources available for remote access. Written approval from an Office Director is required, as well as approval from the Office of Information Technology.

Policy

It is the responsibility of Diocesan employees, contractors, vendors and agents with remote access privileges to the Diocesan corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to the Diocese.

General access to the Internet for recreational use by Diocesan employees and household members through the Diocesan Network on personal computers is strictly prohibited. The employee bears responsibility for all consequences should remote access be misused.

Requirements Respecting Remote Access

The following are requirements regarding remote access to the Diocesan network:

1. Secure remote access must be strictly controlled. Control will be enforced via username and password.

2. Diocesan employees and contractors with remote access privileges must ensure that their Diocesan-owned or personal computer or workstation that is remotely connected to the Diocesan 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.

3. All hosts that are connected to Diocesan internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.

15. Blogging

Use of Diocesan property, systems or computers to add content or make contributions to a blogging website is strictly prohibited unless approved by Senior Management or if it is part of the positions responsibilities ~~y~~. If the job position requires adding content to the blogging website, it should be done in a professional and responsible manner, does not violate Diocesan policy, is not detrimental to Diocesan interests and does not interfere with an employee's work duties.

Employees are personally responsible for the content they publish on blogs, wikis or any other form of user generated media. Be mindful that what you publish will be public for a long time; protect your privacy and those of others. If you publish content to any website outside of the Diocese and it has something to do with work, respect copyright, fair use, financial disclosure and confidentiality laws. Also use a disclaimer such as this: "The postings on this site are my own and don't represent the Diocese positions, strategies or opinions."

16. User Termination

Any user who no longer has a valid business reason to access Diocesan property, systems and personal computer systems (whether due to termination of employment, end of assignment, or otherwise) is required to return to the Diocese all information regarding systems access [including, without limitation, password(s), documentation about system(s), and user manuals and the physical devices themselves]. Such users are prohibited from accessing, or attempting to access, Diocesan property, systems and personal computer systems, using any method after their termination. The Diocese reserves the right to use all legal means to enforce its rights against users that violate the foregoing provisions. The Human Resources department will inform the Office of Technology when an employee is no longer working for the Diocese. Within 30 days from the individual's termination date, the IT Department will back up the home directory and email account, making two copies before deleting the account. This procedure might not apply to temporary staff or consultants.

The Human Resources department will inform the Office of Technology when an employee is no longer working for the Diocese.

17. Confidentiality of Communications

Confidential information of the Diocese must never be transmitted or forwarded to outside individuals or companies not authorized to receive that information. Refrain from routinely forwarding messages containing confidential information to multiple parties unless there is a clear business need.

Reasonable care must be taken regarding discussion or disclosure of confidential and sensitive information in non-secure situations, such as messages left on voice message systems, public telephone conversations, and conversations in open areas.

The following confidentiality notice, or a substantial equivalent, should be attached to the end of e-mail messages to non-Diocese parties.

Confidentiality Notice:

The information in this Internet email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorized.

18. Policy Revisions

All employees of the Diocese shall receive a copy of these Guidelines. Please note that individuals who have previously received the Policy and Procedure Guidelines on Technology effective February 4, 2005, are bound by subsequent revisions of those Guidelines, including any revisions contained in these Guidelines, and are obligated to inform themselves thoroughly of any policy changes.

19. Enforcement

Any individual user found to have violated or to have refused to comply with this policy may be subject to disciplinary action or revocation of technology resource privileges, as well as termination of employment.

20. Reporting Computer Problems

All users are encouraged to report all computer problems (software and hardware) to the Help Desk either by email or by phone. The Help Desk email address is helpdesk@drvc.org The Help Desk hours of operation are Monday through Friday, from 08:30am till 4:30pm. The phone number of the Help Desk is 516-678-5800 ext. 405. If the problem should occur after hours or during the weekend, the user should send an email to the helpdesk, all technicians carry Blackberry devices. If there is an emergency, proper procedures should be followed to alert and notify all parties.