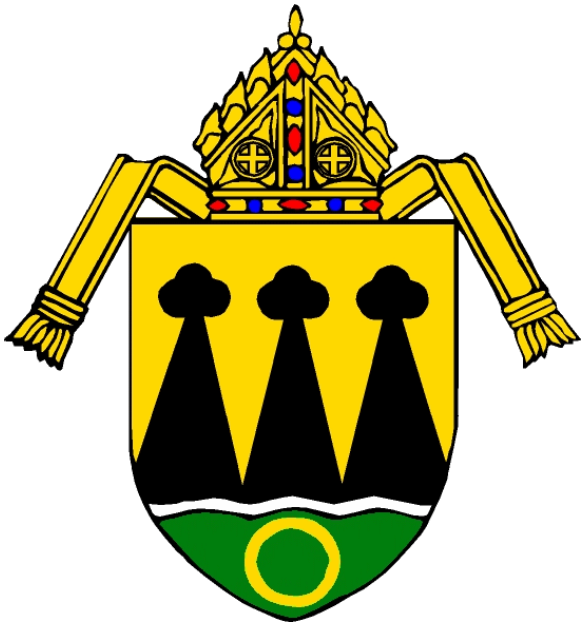
Appendix A



DIOCESE OF RAPID CITY

COMPUTER POLICY

Most Reverend Robert D. Gruss
Bishop of Rapid City

Revised October 2, 2013

COMPUTER POLICY

PURPOSE

The purpose of this policy is to assist the Diocese of Rapid City in protecting its computer system security and assets, to protect the privacy rights of employees, to manage Diocesan resources and to protect the rights of third parties for appropriate access to diocesan files.

POLICY

This document sets forth diocesan policy with regard to access and use of computer hardware, software, data and electronic mail messages. It also sets forth the diocesan policy with regard to disclosure of computer files, created or received, or electronic mail messages sent or received by diocesan employees with the use of the Diocese's computer resources or electronic mail system.

This document sets forth policies on the proper use of computer hardware, software, data and the electronic mail system provided by the Diocese of Rapid City.

The Diocese of Rapid City intends to honor these policies but reserves the right to change them at any time with such prior notices, if any, as the Diocese of Rapid City may deem reasonable under the circumstances.

All employees that utilize diocesan computers are responsible for reading and adhering to these policies. It is the responsibility of supervisors to ensure that each of their employees has received this document and signed a statement of acknowledgment and acceptance of the diocesan Computer Policies.

INTRODUCTION

Information and technology are an integral part of the day-to-day operations of the Diocese of Rapid City. It is the responsibility of diocesan (chancery, parish, mission, diocesan entity, etc.) personnel to protect these resources. The Diocese of Rapid City must take appropriate steps to ensure that information and technology are properly protected and utilized.

The Diocese of Rapid City furnishes its employees, volunteers and other authorized users, hereafter jointly known as “users”, with access to information technology. This includes personal computers, local area networks, remote access capabilities, computer applications, etc., for the purpose of enabling them to fulfill their job and/or ministry responsibilities. This information technology, data and records are the property of the Diocese of Rapid City and are to be used for the Diocese of Rapid City business purposes only.

1. GENERAL

1.1 Storage of Data

1.1.1 Networked Computers: All data shall be stored on network servers in defined storage areas, unless an exception is granted by the Network Administrator for technical reasons.

1.1.2 Non-networked Computers: All data is stored on the local hard drive. If systems become networked in the future, data is to be transferred to the network server. Data should not be stored on removable media except for backup procedures and transporting to other computers systems. See section on portable files below.

1.1.3 Chancery Office: All data shall be stored on network servers. The Network Administrator does not back up the workstation hard drive (the C drive). Also, the process of re-configuring workstations as the environment changes may at any time result in the loss of data stored on the hard drive of the work station. Files placed in the common folder on the server shall be placed in appropriately labeled sub-folders and deleted when no longer needed.

1.2 Backup procedures

Computer software data files are to be backed up on a regular schedule. In general, this consists of full week-day backups of data stored on the server to tape. Archive files on the server will be backed up monthly to tape. Files not stored to the server are to be backed up as appropriate by the user. Typically, detailed backup procedures are documented for the software programs used.

1.3 Management of Files

1.3.1 Responsibilities.

Users of computer systems are expected to manage their computer-generated files. Files should be saved in appropriately named folders to assist in retrieval of those files. Outdated files should be deleted. Permanent files are those files that are used on a regular basis. Following proper backup procedures, deleted files can be recovered if needed in the future. Whether on a stand-alone workstation or a network, consideration must be given in regards to storage space.

1.3.2 Chancery Office:

Because the storage capacity of the network is limited, all users are responsible for deleting outdated files. Files that are older than two years in employees' personal directories and departmental group directories are considered outdated unless they are in a designated archive location. Should the need for space on the server be identified, the Network Administrator will delete any files that are outdated. Users will be notified of this action in advance.

1.3.3 Portable Files:

To facilitate off-site work, employees may copy appropriate files to and from removable media. Appropriate files include word processing documents, electronic spreadsheets and presentation graphic files (examples include files created in Microsoft Office, WordPerfect, Excel, Publisher or PowerPoint). Any removable media which have been used in computers outside of the Diocese of Rapid City must be checked for viruses prior to being used in a diocesan computer. No other files or information may be copied from or to diocesan computers.

1.4 Work Product Ownership

1.4.1 All information developed on a diocesan computer system or introduced to a diocesan computer system is the property of the Diocese of Rapid City, regardless of where it was created.

1.4.2 Likewise, all information developed by a diocesan employee on computers outside of the Diocese of Rapid City, if in conjunction with his or her employment with the Diocese of Rapid City, is the property of the Diocese of Rapid City. Copies of such files must be provided to the Diocese, which has exclusive rights to retain, maintain and modify these files.

1.5 Virus Protection

Computer viruses and other malicious software pose a serious threat to the integrity of both the computer technology and data assets of the Diocese. Collectively referred to as malware, they are designed to be destructive to both computer systems and data. In a networked environment such as exists in the Chancery, the inadvertent introduction of malware to one desktop computer system could result in the infection of every system connected to the network in a matter of moments. Users shall not change their systems configuration or take other steps to defeat virus protection devices or firewall systems.

Individual employees are responsible for verifying that removable media used or received from outside computers are scanned for malware prior to use in diocesan computers. All workstations and servers should be updated with the latest anti-virus protection program and data files. Contact the Network Administrator for assistance in having external media checked.

The Network Administrator will ensure that all diocesan systems are configured with the current standard virus-protection software.

1.6 Configuration

Individual workstations are configured to operate in a complex, networked environment. Users may not change their system setup files. Users who believe their setup files are not configured correctly should contact the Network Administrator for assistance.

1.7 Use

1.7.1 The information system at the Diocese of Rapid City shall be used to conduct diocesan business, except as outlined in section 4, Personal Use of Diocesan Computers.

1.7.2 At the end of the workday, users should log off the network and leave their computers turned on.

1.8 Licensed Software

The Diocese of Rapid City complies with all software copyrights and terms of all software licenses. Diocesan employees may not duplicate licensed software or related documentation. Any such duplication may subject employees and/or the Diocese to both civil and criminal penalties under the United States Copyright Act. Diocesan-owned software may not be loaded on external systems unless the license agreement allows such use and the Network Administrator approves. Also see section 3, SOFTWARE USE AND THE LAW.

2. SECURITY

2.1 Overview

Electronic information is a significant asset of the Diocese of Rapid City. The goal of information system security is to protect information from unauthorized or inappropriate access or modification. The Diocese will maintain a system of information security to protect our proprietary data. Integral parts of this system are the policies, standards and procedures designed for use by users. All users must adhere to these policies, standards and procedures for the complete system to remain viable. These policies, standards and procedures include, but are not limited to: maintaining data confidentiality; maintaining the confidentiality of data security controls and passwords; and immediately reporting any suspected, attempted or actual security violations or breeches.

2.2 Control of Security

Users shall not add additional security, such as passwords, to their workstations or files without the assistance and prior approval of the Network Administrator. Encryption methods should only be used for the transfer of files between two locations. Files should be returned to an unencrypted state following such transmission. Users who believe they have security needs that go beyond current information technology standards and tools should contact the Network Administrator.

2.3 User Access Controls

Computer users shall identify themselves to the system by signing on with their assigned user name. Users shall never attempt to sign on to the system with any other user name. All users shall maintain passwords as required by the Network Administrator. Passwords shall not be shared with anyone for any reason. If a user forgets his or her password, the Network Administrator will facilitate assigning a new password. It is the responsibility of the individual to remember his or her password. All users continue to have an obligation to protect the

confidentiality and nondisclosure of proprietary, confidential and privileged data as well as personally identifiable information, whether communications occur through diocesan computers systems or otherwise. If in doubt about whether an electronic transmission would violate an obligation of confidentiality or nondisclosure, a user must seek advice from his or her supervisor, department head and/or legal counsel identified by the Chancery.

2.4 Access to Data

The users' ability to view, add or modify information in network files is based on access rights configured by the Network Administrator. These can be changed as needed. The Diocese of Rapid City prohibits the use or alteration of diocesan data and/or technology without proper authorization. Contact the Network Administrator to request changes to user access rights.

3. SOFTWARE USE AND THE LAW

3.1 In addition to authorized roles regarding software, the legal implications for improper handling of software can be significant:

3.2 According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000 per work copied, plus criminal penalties, including fines and imprisonment. The Diocese of Rapid City does not condone the illegal duplication of software or any other form of criminal activity. Employees who engage in such activity are also subject to discipline pursuant to diocesan personnel policies.

3.3 All software to be used on diocesan computer systems is to be installed by the Network Administrator or his/her designated representative. Users are prohibited from installing or running software on diocesan systems without prior approval of the Network Administrator. This includes software available for paid or free download from the Internet. Users are prohibited from installing software brought in from home, as this is a copyright violation. Conversely, installing software intended for use on a diocesan system on a home computer is a violation of copyright and is expressly prohibited unless expressly authorized in the licensing agreement with the software manufacturer.

4. PERSONAL USE OF DIOCESAN COMPUTERS

4.1 The Diocese of Rapid City restricts personal use of diocesan computers. The email systems are diocesan property and are intended for diocesan business.

4.2 Employees may use assigned computer resources for limited personal use during non-duty hours. Such use is strictly subject to Proper Use and Prohibited Communications guidelines as listed below and includes such items as Internet use, email, word processing and games. The systems are not to be used for employee personal gain, illegal activities or political activities.

4.3 Other organizations and individuals will not use the Diocese of Rapid City computers. Due to the complex configuration of the diocesan network and support issues, this would not be practically possible.

5. PORTABLE COMPUTER USAGE (Chancery Office)

5.1 Portable computer equipment (e.g. laptops, LCD projector, etc.) may be used for diocesan business outside of diocesan facilities and after normal working hours provided these procedures are followed:

5.2 The Network Administrator has first-use priority for the purpose of training of the use of portable equipment which is not specifically designated for another individual or department.

5.3 The Network Administrator must approve other employees' usage of the portable personal computer. All users must attend a portable computer training session and demonstrate proficiency in the operation of portable computers. Employees may not check out a portable computer prior to receiving this training, as lack of proficiency could result in damage to the portable units.

5.4 Portable computers will be checked out on "first come, first serve" basis. The Network Administrator will monitor this process.

5.5 All employees who make use of diocesan portable computers must read and sign the Employee Portable Computer Agreement. The Network Administrator will ensure that this is done.

5.6 Lost, damaged or stolen portable computer equipment

5.6.1 If a portable computer is lost, damaged or stolen while outside of diocesan facilities, an insurance claim should first be submitted to the individual's insurance company.

5.6.2 If the insurance company of the individual pays for the theft, the check should be signed over to the Diocese and given to the Finance Office.

5.6.3 If the insurance company does not pay, the letter of denial should be forwarded to the Finance Office.

5.6.4 In any case, the individual will not be held responsible for theft. However, it is to be understood that all users of diocesan portable equipment shall take reasonable and appropriate measures to safeguard the security of diocesan property.

5.7 An employee may use diocesan portable computers only for diocesan work and in conformance with Section 4, Personal Use policy.

6. ELECTRONIC MAIL AND OTHER PRIVACY ISSUES

6.1 The Diocese of Rapid City provides and maintains an electronic mail (email) system for the purpose of communicating through written, electronically transmitted form with each other and others outside the Diocese of Rapid City. Email is specifically for users and intended for authorized business purposes only.

6.2 Tact counts. If there is any doubt whether email is the right medium for a message, another form of communication should be used.

6.3 Supervisors should never deliver a reprimand via email.

6.4 Gossip, personal information about anyone and emotional responses to business memos are not appropriate in diocesan email.

6.5 The use of insensitive language or remarks which are derogatory, offensive or insulting is subject to discipline per diocesan personnel policies and practices.

6.6 The use of harassing language, including sexually harassing language or any remarks that may be misinterpreted as such, is subject to discipline per diocesan personnel policies and practices.

6.7 Email is not confidential and may be reviewed at the discretion of the Network Administrator on request from a Department Head.

6.8 The Network Administrator will administer a deletion of email messages as needed to maintain storage capacity on diocesan network servers. Users will be notified of deletions prior to the actual deletions taking place.

6.9 Email should be checked at least daily unless the individual is away from the office.

7. INTERNET USE

7.1 The use of the Internet during work hours should be limited to those subjects that are directly related to an individual's job duties for the Diocese of Rapid City. Employees are advised to exercise discretion when using the Internet since any use can be monitored by individuals outside the organization and may be monitored by the Network Administrator if abuse is suspected.

7.2 The primary function of the computer system is to assist in service delivery to our employees.

7.2.1 To that end, employees may access web sites for work-related research as needed.

7.2.2 This use is limited to web sites that are considered appropriate and employees are expected to exercise good judgment when accessing sites.

7.2.3 Employees may not intentionally access any site that is inappropriate for the Diocese of Rapid City or which could cause embarrassment to the organization or the employee. If this occurs, employees are expected to notify their Department Head.

7.2.4 The Diocese of Rapid City is held to a high standard of scrutiny and ethical behavior. Some examples of inappropriate sites include adult entertainment, sexually explicit material, web sites promoting violence or terrorism, illegal use of controlled substances (drugs) and intolerance of other people/ races/ religions, etc.

7.3 Files downloaded from the Internet should be considered appropriate, according to the above guidelines. If such files need to be taken off premise for any reason, the preferred method is to

electronically email the file(s) to the other location if possible. If that is not possible, files can be transferred to removable media. After being transported to other locations, files should be deleted from removable media.

8. ELECTRONIC COMMUNICATIONS

8.1 Definition

Electronic communication is any message or data sent or received electronically.

8.2 Proper Use

The electronic communications systems are diocesan property and are intended for diocesan business. The systems are not to be used for employee personal gain, illegal activities or political activities. All data and other electronic messages within these systems are the property of Diocese of Rapid City.

8.3 Prohibited communications

Examples of prohibited communications include, but are not limited to:

- Communications, material, information, data or images prohibited by legal authority as obscene, pornographic, sexually explicit or offensive, threatening, abusive, harassing, discriminatory or in violation of any diocesan policy or contrary to the mission or values of the Diocese, including disparagement of others based on race, national origin, marital status, sex, age, disability, pregnancy, religious or political beliefs or any other condition or status protected by federal, state or local laws.

- Communications, materials, information, data or images that may constitute verbal abuse, libel or slander, defamation, fraud or misrepresentation or trade disparagement of users, customers, clients, competitors, vendors or any other person or entity.

- Accessing, viewing, printing, storing, transmitting, disseminating or selling any information protected by law or subject to privilege or an expectation of privacy.

- Accessing, creating, distributing or soliciting sexually oriented messages or images, unwelcome sexual advances, requests for sexual favors or other unwelcome conduct of sexual nature.

- Any attempts to access, monitor or disrupt information that is restricted, confidential or privileged and to which the individual has not expressly been authorized access.

- The intentional or diligent introduction of a computer virus into the system or causing damage to data or the system.

- Granting access to unauthorized persons, either by intentional action such as disclosure of account information or unintentional action such as failure to log off.

- Unauthorized removal, deletion or duplication of data, software or hardware upon a user's termination or departure from the Diocese.
- Violations of software license agreements.
- Development or use of unapproved mailing lists.
- Use of technology systems for private business purposes unrelated to the business of the Diocese of Rapid City.
- Academic dishonesty. (For example, plagiarism)

8.4 Unintentional Access to inappropriate materials

In the event any diocesan employee or personnel unintentionally accesses any inappropriate or pornographic materials, or unintentionally participates in any prohibited communications under §8.3, the diocesan employee or personnel must immediately notify their supervisor so that any necessary corrective action may be taken.

8.5 Privacy

As a matter of routine, the Diocese will not monitor email, voice mail messages or facsimiles. However, the Diocese, through its managers, supervisors and the Network Administrator, reserves the right to review the contents of employees' email, voice mail files or facsimiles. Also, employees may not intentionally intercept, eavesdrop, record, alter or receive other persons' email or voice mail messages or facsimiles without proper authorization. See section 9 regarding Right of Inspection.

8.6 Sensitive Issues

The electronic communications systems should not be used to transmit sensitive material such as personnel decisions, reprimands or material that is confidential in nature. Language that is insensitive, insulting, offensive, derogatory, harassing or discriminatory should be avoided. If there is any doubt whether electronic communication is the proper medium for a message, another form of communication should be used.

8.7 Deleting Messages

Generally, email and voice mail messages are temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of the message, it may be considered a more formal record and should be retained pursuant to a department record retention schedule, as applicable.

8.8 Email Address (Chancery)

To facilitate use of the email system, a user may provide his or her individual email address to professional associates, vendors and other business contacts. An individual's email address at the chancery office is generally formatted in this way: first name initial (no space) last name @

diorc.org. For example: John Doe would be jdoe@diorc.org.

8.9 Junk email (Spam)

8.9.1 The network firewall is designed to reduce the amount of unsolicited email traffic in the network.

8.9.2 Users are asked to delete junk email as soon as possible.

8.9.3 Users may request that the Network Administrator set the firewall to block mail from a particular address or domain if normal attempts to be removed from an email list are ignored by the sender.

8.9.4 If it is not possible to block that address or domain (i.e., If there are other users in the network who need to receive mail from that address) users are encouraged to use the junk mail setting of the program to segregate email from a specific address or with specific content. Employees who are not sure how this is done may ask the Network Administrator for assistance.

8.10 Chain Letter email

Users are required to delete chain letter email messages without forwarding them. These are email messages which arrive with any type of message and request that the receiver "pass it on" to others. These messages serve to clog email servers and are generally unrelated to diocesan business. If an acquaintance routinely forwards such communications, users are asked to contact them and inform them that such messages should not be sent to the diocesan email address.

8.11 Virus Warnings

Users are asked not to forward virus warnings. Most of these messages are hoaxes and should be treated as junk mail. A virus warning that appears to be legitimate may be forwarded to the Network Administrator for investigation. When a significantly threatening virus is being circulated, the Network Administrator may at his/her discretion, send an informational notice to employees.

9. Right of Inspection

9.1 The Diocese of Rapid City reserves the right to inspect and examine any diocesan-owned or -operated communications system, computing resource and/or files or information, including personal computers, area networks, applications and email, contained therein at any time. Users have no privacy right to any data, information or documents received or disseminated on the network or through email. By utilizing these diocesan systems, users consent to the right of the Diocese to inspect and examine all data, information, documents and email.

9.2 When a user acts inappropriately through the technology system, the Diocese reserves the right to report such actions to any outside authorities and/or take appropriate internal diocesan disciplinary action.

9.3 Individuals servicing computers in the State of South Dakota are required by law to report to the authorities any suspected violations of child pornography laws. (State of South Dakota statute 22-22-24-18.)

9.4 When sources outside the Diocese request an inspection and/or examination of any diocesan-owned or -operated technology system, computing resource and/or files or information contained therein, the Diocese will treat the information as confidential unless any one or more of the following conditions exist:

- When approved by the appropriate diocesan official(s) to whom the request is directed;
- When authorized by the owner(s) of information;
- When required by federal, state or local law; or
- When required by a valid subpoena or court order.

Note: When notice is required by law, court order or subpoena, users will receive prior notice of such disclosures (viewing information in the course of normal system maintenance does not constitute disclosure).

10. REMOTE ACCESS

10.1 The Diocese of Rapid City ("Diocese") reserves to itself the unilateral right to grant or not to grant remote access rights to users for e-mail access only or for e-mail and network access. Users of the e-mail and/or network system by remote access, whether by VPN client, internet or e-mail forwarding, are subject to the same policy guidelines as for in-office users.

10.2 No diocesan employee shall have a right to privacy, of any kind, in remote e-mail or internet access to a diocesan-owned or -operated communications system, computing resource and/or files or information including personal computers, area networks, applications and e-mail, if such remote e-mail and/or internet access is granted by the Diocese. Therefore, the Diocese reserves to itself the unilateral right to terminate any employee's remote access privilege at any time. The diocese may terminate any such employee's remote access privilege without cause, reason or explanation.

10.3 Remote access to the diocesan network poses additional confidentiality risks. Users requesting remote access privileges must justify in writing their need for this service. Assurance must be demonstrated that their home computer systems meet the security and confidentiality standards established by the diocese as outlined below or in any other part of this policy.

10.3.1 Home computers used for remote access to diocesan systems via VPN must be equipped with a router which meets the specifications determined by the diocesan technology consultant. The diocesan technology consultant or his designee will install the appropriate software on home computers used for remote access via VPN.

10.3.2 Any home computer used for remote access to diocesan systems must be password protected regardless of whether the user lives alone or with other family members. If other family members are present in the household the user must have a password protected account which only he/she accesses. Under no circumstances are passwords to be shared with anyone nor are passwords to be saved in the computer.

10.3.3 In the event the home computer or laptop is lost or stolen the user must report such loss to the network administrator. Likewise if the home computer or laptop is given away, sold or disposed of, it is of utmost importance that pathways to the diocesan e-mail or network system are removed in a manner in accordance with the direction of the network administrator.

10.3.4 The user must log out of remote access when he/she is not physically working on e-mail or the network. It is not permissible to leave the remote access up and running on a computer that is not physically under the user's control as this constitutes a violation of acceptable confidentiality standards.

10.4 Use of remote access to e-mail and/or the network system is not intended to be used as an alternative to working in the office on designated work days.

10.5 Violation of the terms of remote access privileges is serious and will result in disciplinary action including the possibility of dismissal.

Statement of Acknowledgment and Acceptance of the Diocese of Rapid City Computer Policy

I have received the Diocese of Rapid City Computer Polices, updated October 2, 2013.

I understand that these policies represent the general guidelines for computer use by employees of the Diocese of Rapid City.

I acknowledge that the handbook contains, but is not limited to, the following policies: proper use of computer hardware, software, data and the electronic mail system provided by the Diocese of Rapid City.

I understand that the policies may change without notice. I also understand that it is my responsibility to address questions or request clarifications about the computer policies to my supervisor or the Network Administrator.

Please Print:	
_____	_____
Name	Office
Please Sign:	
_____	_____
Name	Date

PO Box 678 • 606 Cathedral Drive • Rapid City, South Dakota • 57709-0678
(606) 343-3541 • Fax (605) 348-7985 • chancery@diorc.org