



Electronic and Computer Policy

With the rapidly changing nature of electronic media, this policy cannot establish rules to cover or anticipate every possible situation. This policy is intended to express the Diocese of Des Moines' philosophy and establish general principles to be applied in the use of electronic media and services on our property and with diocesan owned devices.

General Use and Ownership

The equipment, services, and technology provided remain at all times the property of the Diocese of Des Moines. All information stored, transmitted, received, composed or contained in the diocesan Information System is the property of the Diocese of Des Moines.

For security and network maintenance purposes, authorized individuals within the Diocese may monitor equipment, systems, and network traffic at any time. Employees should not expect that any communication or information located on or transmitted using diocesan technology will be private or confidential as the Diocese has an obligation to monitor use of its technology.

Employees are expected to limit their computer use to diocesan business-related issues. Appropriate, reasonable, personal use will be allowed during the employee's personal time, such as lunch hours and/or before and after the normal workday. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

Internet and Email Usage

All activities must be appropriate, presenting a positive, professional image of both the employee and the Diocese of Des Moines. There should be no expectation of privacy. Communication that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, defamatory, obscene, threatening, or harassing.

Users must ensure that their conduct in public forums, email, and the Internet conforms to the teachings of the Catholic Church.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited.

All users connected to the network have a responsibility to conserve computer resources such as bandwidth and storage capacity of the Diocese of Des Moines. The user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-work-related uses of the Internet.

The Diocese of Des Moines reserves the right to review, audit, intercept, access, and disclose all messages created, received, or sent over the electronic mail system for any purpose. Employees should have no expectation of privacy in anything they create, store, send or receive using the Diocese of Des Moines computer equipment. The use of encryption of information is recommended when possible.

Social Networking sites

The accessing of social networking sites is permitted for business related issues. Two primary values should be followed when using social media:

1. Visibility
2. Accountability

Diocesan sites require adherence to these following guidelines:

1. When setting up a diocesan social media site, approval from the Director of Communications is required. All usernames and passwords of diocesan social media sites must be provided to the Communications Department.
2. Abide by diocesan guidelines.
3. Identify yourself.
4. Abide by copyright, fair use & disclosure laws.
5. Do not divulge confidential information to others.
6. Do not cite others, post photos or videos, link to another's materials, without their approval.
7. Practice Christian charity
8. Obtain parental permission of a minor before communicating with them via social media. Provide parents the opportunity to be copied on all material sent to their children via social media (includes text messages). No employee should initiate the "friending" of a minor. Minors must make the initial request.
9. Before posting photos of minors, have the consent of parents or school officials.
10. Diocesan social networking sites should be regularly updated. As with any ministry effort, there should be an intentional plan and a set of goals regarding establishing and maintaining a web presence.
11. Report "unofficial" sites that carry the diocesan logo to the diocesan Communications Department.

Personal Communications:

- a. Do not use personal sites for diocesan programs.
- b. Personal communication reflects the Church.
- c. Personal social media sites should also reflect Catholic values.

Remote Access

Remote Email Access: The user is expected to safeguard their diocesan email account when accessing it through the internet from a remote location. All items addressed and implied in this document also apply to accessing email accounts remotely. 2FA (2 Factor Authentication) or MFA (Multi-Factor Authentication) must be used.

Security

The Diocese of Des Moines restricts access to its computing resources and requires that users identify their accounts with a username and password. Sharing user accounts with people other than the Technology Department Staff is prohibited. If there is a breach with user accounts and/or passwords, it will be tracked back to the employee and the employee will be held responsible.

The employees must safeguard their network connection. Steps should be taken to set computer to “Stand-by” mode if the employee will be away from his/her computer for an extended length of time. A username and password are required for the computer to become operational again from the Stand-by mode. The employee should log off the network when leaving his/her computer for the workday.

Violations of this policy, including breaches of confidentiality or security, may result in suspension of electronic communication privileges, disciplinary action up to and including termination, and civil and criminal penalties under state and federal laws.

Loading and Installing Computer Software Policy

Computers shall not be loaded with any programs or files that have not been purchased for that specific computer by the Diocese of Des Moines. No files shall be downloaded from the Internet or any files accepted from an E-mail message. The exception to this would be files from other computers or files from business associates of the Diocese of Des Moines.

In order to resolve problems and to reduce conflicts with hardware and software on PCs, all software and hardware must be approved by the department head in consultation with the IT Department prior to the purchase and installation of the product. Software and hardware that is not approved and/or not used to conduct business will be removed. This includes backdrops, screensavers, and unapproved personal software.

If a computer is not operating properly, contact the IT Department. The IT Department will check the computer to see if it is a network, software or hardware problem. If the computer needs service, that office will then coordinate the unit’s repair and return of the computer to the employee.

Security Awareness Training

Security and privacy awareness and training are important aspects in protecting the confidentiality and integrity of sensitive information. Employees are the first line of defense and must be made aware of the security risks associated with the work performed at the Diocese of Des Moines.

All employees, contractors, and anyone accessing Diocese of Des Moines information systems must understand how to protect the integrity of information and information systems.

The Diocese of Des Moines will ensure that all employees and contractors are given security and privacy awareness training during the new hire process. This training reflects common security and privacy awareness specific to the Diocese of Des Moines environment including, but not limited to, physical access, restricted areas, potential incidents, how to report incidents, laptop best practices and how to spot a phishing scam. New hire security training must be completed within one week of employee start date.

The Diocese of Des Moines will conduct refresher training on a regular basis for all employees and at any time there are significant changes to the environment. This will be administered via our current security awareness training company and tracked for completeness and passing grade to show adequate understanding of the material.

All employees and contractors are responsible for understanding and following all security-related policies and procedures, and asking their manager or Technology Coordinator for clarification if needed.

Managers are responsible for ensuring all employees complete required security training. The Technology Coordinator is responsible for enrolling all employees in first-time and ongoing security training and tracking results.

Compliance

Compliance with the policy defined in this document is mandatory. Failure to comply with this Electronic and Computer Policy may result in disciplinary actions up to and including termination of employment. Failure to comply with this Electronic and Computer Policy may result in termination of contracts for contractors, partners, consultants and other entities. Legal actions may also be taken for violations of applicable regulations and laws.