Electronic Communications - Acceptable Use Policy

The Catholic Diocese of Richmond's goal in establishing policy for the use of communications technology is to increase productivity and improve communication among diocesan, parish, school, and other diocesan personnel; to communicate and provide information to a larger audience; and to allow access to the wealth of information available on the Internet.

The use of the word(s) Diocese or Diocesan throughout this policy covers all employing locations of the Catholic Diocese of Richmond. These policies apply to employees, contractors, volunteers and others granted access to Diocesan systems.

The Diocese owns all computer hardware and software, networks, user accounts, e-mail and voice mail facilities, all internal and external messages and files created, sent, received or stored on any computer system and network, unless otherwise protected by a valid copyright.

Consistent with the Diocesan Code of Ethics, employees must adhere to the highest ethical/legal standards when using various communications.

Section One: General, Computing Policy

The Diocese reserves the right to retrieve and review any message or file composed, sent or received. It should be noted that although a message or file is deleted or erased, it is still possible to recreate the message. Therefore, privacy of messages cannot be assured to anyone. Although electronic mail and voice mail may allow the use of passwords for security, confidentiality cannot be guaranteed.

In order to ensure smooth system operations, the system administrator, as designated by the employer for each employing location, has the authority to monitor the specific location's accounts. A user must abide by the terms of all software licensing agreements and copyright laws. Once a user receives a user ID, he/she is solely responsible for the actions taken while using that ID. Limited casual, personal use of systems will be regulated by the user's supervisor, and is considered acceptable except for activities as are noted elsewhere in this document.

The following are prohibited actions for users:

1. Sharing your user ID with any person.
2. Deleting, examining, copying, or modifing files and/or data belonging to other users without their consent.
3. Using facilities and/or services for commercial purposes.
4. Any unauthorized, deliberate action which damages or disrupts a computing system, alters its normal performance, or causes it to malfunction is a violation, regardless of system location or time duration.
5. Copying personal programs onto Diocesan owned equipment or network systems without the consent of the designated system administrator.
6. Copying programs owned by the Diocese for personal use.
7. Abusing computer equipment.

The designated parish or school system administrator should receive additional guidance regarding appropriate usage for accessing networks from the location's employer with support from the Diocesan Office of Information Technology.

Section Two: Internet Access

The Internet is an open network in both implementation and spirit. Technical measures could be invoked to constrain Internet use, but they would limit the utility of the Internet. The policy does not attempt to articulate all required or proscribed behavior by its employees. Instead, each employee's judgment of appropriate conduct is relied upon. To assist in such judgment, the following general guidelines are offered:

1. Use of the Internet through diocesan accounts must be in support of the work of the Church and the Diocese.
2. Users are prohibited from posting, transmitting or downloading any unlawful, threatening, abusive, libelous, defamatory, obscene, pornographic, or profane information of any kind, including without limitation, any transmissions constituting or encouraging conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state or national regulations.
3. Any use of diocesan e-mail accounts or web sites for commercial purposes or partisan political lobbying is prohibited.
4. No use of the Internet shall serve to disrupt the use of the network by other users.
5. All material viewed on web sites should be considered copyrighted and not available for reproduction, unless specifically stated otherwise or unless specific permission is granted for reproduction.
6. Diocesan e-mail accounts should be used only by the authorized user(s) of the account for the authorized purpose. Passwords allowing entry into secured sections of the diocese's web site should be used only by authorized personnel.
7. All communications and information accessible via the Internet should be assumed to be private property. Users should also make every effort to validate information and sources, and obtain permission for use, before posting, and to list sources when passing along information received.
8. Users are strongly encouraged to maintain virus protection software on their computers.
9. Schools and any other entities that allow children to have access to the Internet must have safeguards to ensure that children cannot access inappropriate material.
10. NEVER reveal or divulge any personal information, such as your address, phone number, password, or social security number.

The use of the Internet is a privilege, not a right. If inappropriate use is discovered, it can result in a cancellation of those privileges and may lead to additional disciplinary action, up to and including termination.

Section 3: Social Networking Guidelines

Social networking has revolutionized the way people communicate and share information with one another. The term social networking includes, but is not confined to the use of blogs/wikis, message boards/forums, FaceBook, MySpace, Twitter, LinkedIn and other posting technologies such as YouTube, Picasa, Flickr, etc. The guidelines serve to assist employees with the use of social networking:

1. When establishing a social network account it is recommended it be set up in the name of the church, ministry, or school – and independent of any one person's personal social networking account. In addition the logon information for that account should be documented and kept on file.
2. Before launching any social networking project, it is expected that the pastor/principal/office director approve the project, evaluate its appropriateness in ministry and determine who will develop and who will oversee its use.
3. In order to be inclusive and fully transparent, locations utilizing social networking media are expected to inform all interested parties of this new form of communication. This can be accomplished via a bulletin, newsletter, website, etc.
4. Any information reflected on a social network page for the parish/school/ministry should also be reflected on the parish/school website, so that the information is accessible in both areas.
5. No pictures/images/videos/logos should be tagged or linked without permission. Pictures of individuals should have the written permission of the individual.
6. Pictures of minors should always have the written permission of parents/guardians and should never include names or other personal information about the individual. Pictures of minors are not to be tagged as this could direct individuals away from the parish/school/ministry site and to the personal page of an individual.
7. The administrator/owner should monitor conversations, wall postings, images and the behavior of members of the group and challenge, educate, intervene and/or delete as necessary.
8. No employee should initiate the "friending" of a minor. Minors must make the initial request.
9. It is recommended that employees use caution when "friending" others. Employees accept responsibility when accepting an individual on a ministerial page.
10. Employees are expected to write knowledgeably, accurately, and use appropriate professionalism. Employees should communicate using their official location related email address.
11. Employees are not to provide a link or otherwise refer to the Diocesan website on their personal website, social networks or weblogs.
12. While the Diocese respects the rights of employees regarding their personal life outside of business hours, the following *recommendations* are provided:
    - All employees who have personal social networking accounts should maintain boundaries between their personal and professional lives.
    - In the event that you identify yourself as an employee of the Diocese on a personal website, weblog, or social network, it is recommended that the following notice be placed in a prominent place on your site: "*The views expressed on this website/weblog/social network are mine alone and do not necessarily reflect the views of my employer*."
    - If you serve in a leadership role in the Diocese, consider whether it is appropriate to be a friend on a social networking page of a parent, student, parishioner or other individual who interacts with you only through this leadership role. It is recommended that individuals not friend minors that are known primarily through a Diocesan relationship.