§4500 ELECTRONIC COMMUNICATIONS

The Diocese of Springfield in Illinois, its affiliated agencies, offices, Juridic Persons, Catholic Parishes and Schools within its borders use many forms of communication and information technologies.[1] These technologies, when properly used, support our business and pastoral activities and enable closer and timely communication within the Diocese and with our constituents. There is a continuing evolution of associated laws and conventions governing acceptable use and careless use of electronic communication tools that can have dramatic consequences, harming the Diocese, our constituents, and our clerics/employees/volunteers. These policies are intended to minimize the likelihood of such harm by educating our clerics/employees/volunteers and by acting as the basis for written policies and procedures whose existence will serve to protect the Diocese in litigation and other disputes. Access to Diocesan communications tools is provided in conjunction with the Diocese's business and clerics/employees/volunteers job responsibilities. clerics/employees/volunteers use of these tools is subject to this policy and other Diocesan policies and procedures. This policy is binding for all Diocesan and agency clerics/employees/volunteers. Diocesan communication tools also may be made available to individuals who are not Diocesan staff (e.g., consultants, vendors, committee members, temporaries, and volunteers). Use of these tools by such persons is subject to this policy.

§4501. USE AND MISUSE OF COMMUNICATION TOOLS

Definition:

"Communication tools" include, but are not limited to, e-mail, internet, computers, tablets, cell/smart phones and voicemail.

[1] An "agency" as used herein shall include any department, institution, office, parish, school, Juridic person or any subdivision thereof governed by the moral authority of the Roman Catholic Bishop of Springfield in Illinois. (The authority to determine policies for these entities is stated in the, **2017 Diocesan Synodal Statues, Part I, General Norms #9**, *"Diocesan policies further specify and delineate in greater detail the fundamental particular laws of these statutes and require all diocesan, parish and Catholic school personnel to act in a prescribed manner in handling specified situations. Diocesan procedures are uniform methods or standards of implementing diocesan policies."*)

§4501.1. OWNERSHIP AND ACCESS

4501.1.1. ***Policy.*** Communications tools purchased or provided by the Diocese or an agency for use in the performance of its business are Diocesan/agency property and subject to reasonable inspection. All information created in-the-course-of Diocesan/agency business and/or produced or carried on Diocesan/agency communications tools is likewise Diocesan/agency property and subject to reasonable inspection.

4501.1.2. ***Policy.*** Each user accessing these tools must have a unique user ID assigned by the system administrator (i.e. IT director). Each user must have a unique password. **Under no circumstances shall it be permissible to allow another person to use one's ID or password**.

§4501.2. ACCEPTABLE USE

In-the-course-of their employment, clerics/employees/volunteers may use these tools to communicate internally with Diocesan coworkers or externally with parishes, agencies, consultants, vendors, and other professional and business acquaintances. The Diocese provides staff with electronic communication tools to facilitate business communications and to enhance productivity.

4501.2.1. ***Policy.*** As with the telephone, there may be occasions to use these communication tools for personal purposes. Personal use is permitted so long as it does not interfere with the job performance, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other staff members.

4501.2.2. ***Policy.*** Under no circumstances shall such communication tools be used for personal gain, or to solicit others for activities unrelated to the Diocese's business, or in connection with political campaigns or lobbying.

4501.2.3. ***Policy.*** Employees or volunteers may not use any communication tool:

(1) to carry or transmit defamatory, discriminatory, or obscene material;

(2) to infringe upon another person's intellectual property rights (e.g. copyrights);

(3) in a manner that violates the terms of any applicable telecommunication license or any laws governing transborder data flow (e.g., laws dealing with data collection, protection, privacy, confidentiality, and security); or

(4) in connection with any attempt to penetrate computer or network security of any company or other system, or to gain unauthorized access (or attempted access) to any other person's computer, email or voicemail accounts or equipment: or in connection with the violation or attempted violation of any other law.

§4501.3. INTERNET USE

The Diocese is aware that web "surfing" may be business-related and serve a legitimate business function, but the potential for abuse exists. The Internet provides access to a huge amount of information and resources that can greatly enhance our ability to deliver services to our constituents. Today there is no single, comprehensive directory of resources available for the Internet and users sometimes must "navigate" through much unneeded information to reach useful material.

4501.3.1. ***Policy.*** The Diocese encourages exploration of the Internet for legitimate business-related or professional activities, but staff shall not "browse the web" on Diocesan time, create personal "Home Pages", or otherwise use Diocesan/agency facilities to access Internet sites for reasons unrelated to Diocesan/agency business and clerics/employees/volunteers job responsibilities.

§4501.4. REPRESENTING THE DIOCESE IN STAFF POSTINGS

Any information published electronically (sometime called a "Posting") is a reflection on the Diocese of Springfield in Illinois. Despite disclaimers that may be made (e.g., that views belong to a particular individual and may not reflect those of the Diocese) readers elsewhere may make the association between a posting and the Diocese of Springfield in Illinois. clerics/employees/volunteers *should be aware that true anonymity is very difficult to obtain when using these tools. While Internet blogs, newsgroup visits, and net "surfing" sometimes appear to be done anonymously (e.g., by employing pseudonyms), accessing such services/servers through the Diocese's network facilities normally leaves an "audit trail" indicating at least the identity of the Diocese's proxy/server (and may leave an audit trail pointing directly to an individual). Inappropriate use of Diocesan facilities may damage the Diocese's reputation and could give rise to corporate and individual liabilities.*

4501.4.1. ***Policy.*** Clerics/employees/volunteers shall make every effort to be professional in all usage of Diocesan/agency communication tools and ensure that information is correct before posting any article or opinions.

4501.4.2. ***Policy.*** Clerics/employees/volunteers shall use a disclaimer that the opinions offered are their own and do not necessarily reflect the opinions or position of the Diocese of Springfield in Illinois.

§4501.5. UNACCEPTABLE CONTENT

Although the Diocese does not regularly monitor voicemail or electronic messages, clerics/employees/volunteers should be aware that even personal mail and voicemail messages may be viewed publicly or by Diocesan management without further notice.

4501.5.1. ***Policy.*** Under no circumstances shall any posting, voicemail or email originating at the Diocese be in violation of the teachings of the Catholic Church, the letter or spirit of the Diocese's Equal Employment Opportunity or Sexual Harassment policies, or the restrictions against 501(c)(3) tax exempt organizations (cf. "*Political Responsibility: Proclaiming the Gospel of Life, Protecting the Least Among Us, and Pursuing the Common Good*", United States Catholic Conference, 1995.). Examples of unacceptable content include, but are not limited to:

(1) sexually explicit messages, images, cartoon or jokes;
(2) unwelcome propositions, requests for dates, love letters, profanity, obscenity, slander, or libel;
(3) direct or indirect support for or opposition to any candidate for elective public office;
(4) distribution of campaign literature or biased voter educational material;
(5) publication or transmission of paid political advertising, biased coverage of candidate activity or opinions that endorse or oppose a particular candidate;
(6) endorsements of candidates or political parties;
(7) ethnic, religious, or racial slurs; or
(8) any message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious beliefs.

The standard used to determine whether "sexual harassment" has occurred is whether the recipient could reasonably consider the message to be offensive - - the sender's intentions are irrelevant.

§4501.6. ELECTRONIC FORGERY

Electronic forgery is defined as misrepresentation of identity in any way while using electronic communication systems (e.g., by using another's email account without permission, or so-called IP spoofing, or by modifying another's messages without permission).

4501.6.1. ***Policy.*** Messages written by others shall be forwarded "as-is" and with no changes, except to the extent that staff clearly indicates where they have edited the original message (e.g., by using brackets [ ] or by using other characters to flag edited text).

§4501.7. INTELLECTUAL PROPERTY

4501.7.1. ***Policy***. Clerics/employees/volunteers must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information and intentions. Clerics/employees/volunteers may not copy, use, or transfer others' materials without appropriate authorization.

Procedure

Clerics/employees/volunteers are responsible for being aware that download software and other copyrighted material may be subject to licensing obligations or restrictions. When staff are in doubt, they should contact the Office of Human Services.

§4501.8. ENCRYPTION

4501.8.1. ***Policy***. Diocesan security standards and policies also govern the use of encryption tools. Only authorized encryption tools (software and hardware) may be used in connection with any Diocesan/agency communication tools. Except with the prior written consent of the appropriate IT manager, all such tools must implement key-recovery or key-escrow techniques to permit the Diocese/agency to access and recover all encrypted information (e.g., in the case of the absence of the staff member who performed the encryption).

Procedure

When password protecting files clerics/employees/volunteers shall provide the password in a sealed dated envelope to their supervisor or the IT manager. Encryption recovery keys will be maintained by the IT manager as part of a secure disaster recovery plan. Mobile computing devices such as laptops and smart phone will use full disk encryption in case of loss or theft.

§4501.9. SOFTWARE PIRACY

4501.9.1. ***Policy***. Diocesan/agencies shall not load or use software that they do not own a legally purchased license.

§4502. LIMITS OF PRIVACY

*No electronic communications facility is completely secure. This means that information stored on or carried over Diocesan/agency communications tools may be the subject of accidental or intentional interception, mis-delivery, attack, or authorized Diocesan/agency review. When stored on computers, email messages and other files typically are subject to routine back-up procedures (see **4502.4.1.)**. This means that copies of these files may be retained for long periods of time (in accordance with back-up recycling and document retention procedures). Also, keep in mind that many site-wide backup systems do not guarantee privacy of backup copies (e.g., system administrators may have access).*

§4502.1. RETENTION AND SECURITY OF MESSAGES

4502.1.1. ***Policy.*** Email and voicemail messages, and computer stored items are Diocesan/agency property and business records, and may have legal and operational effect identical to that of traditional, hardcopy documents (for example, that are "discoverable" in litigation, and can be used in evidence). Retention of voice mail logs and email are governed by Diocesan Retention Schedules as outlined in the Diocesan Records Policy. Accordingly, all email messages shall be treated as though others may later view them. **Email should *not* be considered a confidential means of correspondence.**

§4502.2. LIMITED EXPECTATION OF PRIVACY

The Diocese of Springfield in Illinois respects the personal privacy of its staff. However, because communications tools are provided for the Diocese's/agency's business purposes, clerics/employees/volunteers rights of privacy in this context are quite limited. Clerics/employees/volunteers should have no expectation that any information transmitted over Diocesan/agency facilities or stored on Diocesan/agency-owned or leased computers or smart phones is or will remain private. These systems are owned and/or controlled by the Diocese of Springfield in Illinois (or its agencies) are accessible at all times by the Diocese/agency for maintenance, upgrades, or any other business or legal purpose. Clerics/employees/volunteer members who use Diocesan/agency communication tools should be aware that our firewall (and other security tools) creates an audit log detailing every request for access in either direction by each user. Also, in-the-course-of their duties, system operators and managers may monitor employee use of the Internet or review the contents of stored or transmitted data.

4502.2.1. ***Policy.*** The Diocese of Springfield in Illinois permits limited personal use of all these communications tools on the express understanding that it reserves the right (for its business purposes or as may be required by law) to review clerics/employees/volunteers use, and to inspect all material created by or stored on, these communication tools. Use of these tools constitutes the employee's permission for the Diocese/agency to monitor communications and to access files that are made on or with these communication tools.

4502.3. DIOCESAN ACCESS TO COMPUTERS, VOICEMAIL AND EMAIL SYSTEMS

4502.3.1. ***Policy.*** Diocesan/agency management will not routinely examine staff communications or files. However, such examination generally may be expected to occur in the following circumstances (which are not intended to be all-inclusive):

(1) ensuring that Diocesan systems are not being used to transmit discriminatory or offensive messages, or in connection with the infringement or violation of any other person's rights;
(2) determining the presence of illegal material or unlicensed software;
(3) counteracting theft or espionage;
(4) ensuring that communications tools are not being used for inappropriate purposes;
(5) responding to legal proceedings that for producing electronically-stored evidence;
(6) locating, accessing, and retrieving information in an employee's absence; and
(7) investigating indications of impropriety.

4502.4. DIOCESAN COMPUTER MAINTENANCE

4502.4.1. ***Policy.*** Diocesan/agency management will ensure that all computers have operating system (i.e. Windows OS and operational software) and data (records created by software) failure recovery systems (formerly back-up devices) that provide electronic media storage ***offsite*** for operating systems and mission critical data/records. This is necessary in the event of computer hardware failure, or data loss. The sequencing of transferring operating system vs. data offsite storage may be different. Check with the Diocesan IT department for best practices and consultation. Data recovery systems are not for file storage and should only be sequenced for system failure and recovery.

§4503 PENALITES

4503.1. ***Policy.*** Violations of these policies can result in responses ranging from denial of future access, litigation entanglements or, termination of employment.