DIOCESE OF LA CROSSE
INTERNET AND OTHER IT NETWORK USE POLICY

The Diocese of La Crosse, its Parishes, and its Schools (hereinafter "Diocese/Parish/School") provide employees with the opportunity to access its Internet Systems for Diocesan/Parish/School purposes. "Internet Systems" shall mean any Diocese/Parish/School provided devices, Internet connections (including any wireless connections) provided by the Diocese/Parish/School, Diocese/Parish/School e-mail accounts, and any intranet or any remote connection to Diocese/Parish/School systems. Diocese/Parish/School provided devices shall include any electronic devices provided by the Diocese/Parish/School, including, but not limited to, desktop computers, laptops, and any hand-held devices.

This technology is a powerful tool to facilitate communication internally and externally. However, it also presents significant challenges to confidentiality, privacy, and liability requiring the exercise of significant responsibility on an individual basis. Therefore, the following policy shall apply to all employees who use the Diocese's/Parishes'/Schools' Internet Systems.

1. Access to the Diocese's/Parishes'/Schools' Internet Systems is provided as a tool to assist the employee in the performance of his/her duties.

2. Users have no right to privacy while using the Diocese's/Parishes'/Schools' Internet Systems. Diocesan/Parish/School personnel will review files and communications without notice to any users to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files will be private.

3. For all technology personally owned, provided, maintained or paid for by the user there is a general expectation of privacy except to the extent such personal technology is used for Diocesan/Parish/School volunteer or paid for activities or purposes. In such cases, there is no expectation of privacy.

4. Log on and other passwords may not be shared with any third party, nor may they be shared with another employee, unless requested by an immediate supervisor or person in charge.

5. Use of Internet Systems knowingly to disable or overload any computer system or network or to circumvent any system or controls intended to protect the privacy or security of another user is prohibited.

6. Users of the Internet Systems are encouraged to open Internet E-mail messages from reputable businesses you recognize by name and to delete, and not open, messages that are not recognizable. These messages may contain viruses, Trojan horses, worms, bombs, or other malware, that can cause damage to the computer system.

7. Software or files downloaded via Internet Systems or on to Diocese/Parish/School provided devices become the property of the Diocese/Parish/School. Any such files or software may be used only in ways that are consistent with their licenses or copyrights. Employees may not use Internet Systems knowingly to download to distribute pirated software or data. Employees are to obtain permission from the network administrator to download information, files, or software to the Diocese's/Parishes'/Schools' network, as they may contain viruses or have conflicts with programs currently used.

8. The retrieval, display or storage of any kind of sexually explicit image or documentation on any Diocesan/Parish/School system is a violation of our harassment policy. In addition, sexually explicit or offensive material may not be archived, stored, distributed, edited or recorded using Internet Systems. If an employee accidentally connects to a site that contains sexually explicit or offensive material, the employee must immediately disconnect from that site.

9. Employees may not use Internet Systems to download entertainment software or games or play games over the Internet, except for in Schools if preapproved by the school principal for educational purposes.

10. Employees may not use Internet Systems to download images or videos unless there is an explicit business-related use for the material.

11. The following are also specifically prohibited:
    A. Sending or displaying offensive messages or pictures.
    B. Using obscene language.
    C. Harassing, insulting, or attacking others.
    D. Damaging computers, computer systems or computer networks.
    E. Violating copyright law.
    F. Using another person's password.
    G. Trespassing in another person's folder, work or files.
    H. Intentionally wasting limited resources, including the use of "chain letters" and messages, broadcast a mailing list or individuals.
    I. Employing the network for private and personal commercial purposes.
    J. Revealing the employer's personal address or phone number, or the personal address or phone number of any other person without the consent of the individual.

12. Violations of this policy or of law connected with the use of the Internet Systems will result in disciplinary action up to and including termination of employment.

13. Personally owned, used, maintained or paid for technology may be subject to search and/or seizure by the Diocese/Parish/School under the following circumstances:
    A. Upon the receipt of technology related complaints involving child pornography, pornography, or copyright violations.
    B. Technology which contains evidence of other misconduct complaints, including but not limited to improper relationships and/or theft.
    C. In circumstances where a professional assessment has suggested or directed such search.

14. Investigative protocols of complaints of misuse of Diocesan/Parish/School technology include:
    A. The steps:
        (1) A complaint is received
        (2) The Diocese/Parish/School seizes the Diocese/Parish/School equipment without notice.
        (3) An internal Diocesan/Parish/School IT review occurs.
        (4) If necessary, an external IT review occurs.
        (5) If required, report to authorities.

B. The reporting result:

(1) If the IT records contain evidence of child pornography, the matter shall be reported to authorities.

(2) If the IT records contain evidence of an improper child or adult relationship (therapist) a report shall be made to authorities.

(3) If non-child pornography or other evidence of improper conduct occurs, the results may be reported to the authorities depending upon the circumstances.

15. Investigative protocols of complaints of technology misuse of personally owned technology include:

A. The steps:

(1) Receipt of complaint involving the improper use of private technology for Diocesan/Parish/School uses or purposes.

(2) The Diocese/Parish/School seeks the voluntary consent of the volunteer or employee to search personally owned technology.

(3) If consent is granted, then the steps outlined in paragraph 15.A. 3, 4 and 5 above shall be followed.

(4) If employee/volunteer consent is denied such access, the employee/volunteer shall be placed on Administrative Leave pending further investigation, may or may not be suspended without pay and where required, all reports to authorities shall be made.

16. Remedial protocols for misconduct involving either Diocesan/Parish/School owned technology or private technology within the exceptions noted include:

A. Definitions:

(1) "Misconduct" is defined as crimes, Red or Green book violations or violations of other Diocesan/Parish/School policy.

(2) "Determined" is defined as either being admitted or sufficiently confirmed.

B. Consequences of admissions or confirmations:

(1) If possession of child pornography or other crimes involving a child, the person shall be removed, the matter shall be immediately reported to authorities and in all other respects both the Red and the Green books shall be followed.

(2) If misconduct involving technology does not involve child pornography, depending upon the circumstances the person may be removed.

(3) All matters required by law to be reported shall be reported.

(4) In matters not involving crimes, the person may be subjected to random monitoring and/or a permanent monitor of all future technology use.

(5) Measures suggested by professionals may be implemented.