Appendix A

COMPUTER USE POLICY AND GUIDELINES USING SOCIAL MEDIA

COMPUTER USE POLICY

Computers and Internet access must be used in ways which support and enhance the ministries of the Episcopal Diocese of Milwaukee and its congregations. Because we cannot control the content of the information found on other computer systems accessed via the Internet, it is crucial that we use our Internet connections and our computers in ways that are responsible, efficient, ethical, legal, and in support of our shared mission and ministry. The use of computers is a significant benefit to the life of congregations of the Episcopal Diocese of Milwaukee. With these benefits come important responsibilities.

This policy seeks to ensure that the use of computers and Internet access on the properties of the Episcopal Diocese of Milwaukee and its congregations, shall be in support of our mission and ministry and reflective of our shared values. This policy applies to all on-site users (lay or ordained, paid or volunteer) of computers and all users of Internet access at our parishes and diocesan offices regardless of the owner of the computer or the holder of the Internet Service Provider (ISP) account (such as AOL, Prodigy, and the like).

> Thus, for example, a parish secretary using the office computer to access the Internet via the parish's ISP account must comply with this policy. Similarly, the volunteer who is in a parish classroom using his or her own laptop computer and ISP account must also comply with this policy.

Further, this policy governs off-site use of computers owned by the Diocese or its parishes, as well as off site access to ISP accounts held by the Diocese or its parishes.

All users shall comply with the following general standards when using computers and when connecting with the internet:

1. Behave responsibly when using computers and when connected to the Internet;
2. Comply with all applicable laws, rules and regulations, and with all other (non computer-specific) policies of the Diocese. Respect the rights and property of others, including copyrights and other intellectual property rights.

As a further illustration of these general principles, the following are examples of unacceptable uses of computers and the internet under this policy:

1. Intentionally accessing, viewing, storing, or displaying any site or material that is pornographic, racist, sexist, homophobic, or otherwise offensive, including verbal descriptions, audio files, photography, drawings or paintings, and cartoons;
2. Soliciting sex or purchasing pornographic materials;
3. Creating, transmitting or reproducing language inappropriate to the Christian context, including language which is: profane, abusive, defamatory, degrading, harassing, threatening, or which breaches obligations of confidentiality;
4. Committing forgery, blackmail, identity theft, libel, selling or purchasing illegal substances, or gaining unauthorized access to other computer systems for any purpose (a.k.a. "hacking");

5. Disguising one's identity, impersonating other users, or sending anonymous email messages;
6. Copying or distributing material obtained from the Internet if doing so violates a copyright or other intellectual property right;
7. Copying, deleting or modifying another's files or data without permission;
8. Intentionally accessing, distributing, copying, deleting or modifying another's email without permission;
9. Intentionally damaging computer equipment, files, data, or networks;
10. Intentionally accessing or transmitting computer viruses or other harmful files, or otherwise intentionally damaging computer equipment, files, data, or networks;
11. Commercial uses (including selling or buying anything for personal financial gain and conducting personal for-profit business activities).

GUIDELINES USING SOCIAL MEDIA

Social media now accounts for the largest share of internet usage, surpassing even email. It is essential that the church be present in this mission field, as it has changed the internet from a place where people go to find information, to a place where people meet in virtual community, expecting to share their lives, thoughts, and their beliefs with others.

In churches, social media and email can promote nearly viral outreach, deepen the real life sense of community at a church, and build a feeling of week-long togetherness. But just like real-life relationships and interactions, digital communications need to be lived into with the appropriate boundaries to protect yourself and others.

The following recommendations and guidelines for web and social media use are in alignment with the Diocese of Milwaukee's accepted principles of healthy boundaries and safe church practices.

Commonly Accepted Principles of Healthy Boundaries and Safe Church

1. Adults have more power than children and youth
2. Clergy have more power than people with whom they have a pastoral relationship.
3. The mutuality of friendship cannot exist when there is a disparity of power.
4. Two unrelated adults must be able to maintain visual contact with each other any time they engage in ministry with children or youth.
5. Windows in doors allow transparency of interactions with children, youth and adults who may be vulnerable.

General Information about Digital Communications

1. All communications sent digitally (email, social networking sites, notes or posts, etc.) are NOT CONFIDENTIAL and may be shared or reposted to others.
2. Interactions in the virtual world need to be transparent, as a window in the door provides transparency in the physical world.
3. In the virtual world healthy boundaries and safe church practices must be adhered to as they are in the physical world.

4. In the virtual world, "friend" can mean anyone with whom you are willing to communicate through that medium. In the physical world, friend can mean much more in terms of intimacy, self- disclosure, mutuality and expectations for relationship.
5. Laws regarding mandated reporting of suspected abuse/neglect/exploitation of children, youth, elders and vulnerable adults apply in the virtual world as they do in the physical world.

Recommended Practices and Guidelines for Interactions with Children and Youth: Social Networking Sites-Relationships

1. Adults who minister to children and youth are strongly encouraged to set very stringent privacy settings on any social networking profile.
2. Individual personal profiles are to be used to interact with real friends, family and peers. Adults should not submit "friend" requests to minors or youth. Youth may not be able to decline such requests due to the disparity of power between youth and adults. Youth may ask to be "friends", and adults should discern the level of contact they want to maintain with youth prior to responding to these requests.
3. If an adult chooses to accept friend requests from minors or youth who are associated with their community of faith, other adult leaders must have full access to all aspects of that adult's profile and correspondence.
4. Adults who want to connect via a social networking website with youth to whom they minister are strongly encouraged to set up a closed group page or official organization page that youth may join. Youth requesting to "friend" an adult can then be invited to join this closed group or organization page rather than be accepted as a friend on an adult's personal profile account. The purpose of these two separate accounts/profiles is to create a line of privacy and maintain healthy boundaries with youth and real family, friends and colleagues.
5. Any material on any site (whether affiliated with the church or not) that raises suspicion that a child has been or will be abused/neglected/exploited should be immediately reported to the clergy and to the Department of Children, Youth and Families (DCYF). If the material is on a church affiliated site, that material should be documented for church records and then removed from the site after consultation with authorities.

Recommended Practices and Guidelines for Interactions with Children and Youth: Groups/Organization Pages on Social Networking Sites

1. Clergy and Lay leaders should carefully discuss whether a closed group page or an official organization page would better serve their Social Networking purposes. Consideration of the specific purpose of the group should be given (ex. Confirmation, pilgrimage, mission trips etc.). Privacy and publicity settings are very different depending which you choose.
2. Groups/Organization pages should have at least two unrelated adult administrators as well as at least two youth. Closed groups, but not "hidden" groups, should be used for youth groups (J2A, Rite 13, administrators).
3. Invitations to youth to join a group should be made by youth administrators, unless a youth previously asked an adult administrator to invite him/her to join the group. This is not an issue with official organization pages, as all invites appear from the organization itself rather than an individual.

4. Behavioral covenants should be created to govern what content is appropriate and inappropriate for an online youth group of either type.
5. Any material on any site (whether affiliated with the church or not) that raises suspicion that a child has been or will be abused/neglected/exploited should be immediately reported to the clergy and/or Office of the Bishop. If the material is on a church affiliated site, that material should be documented for church records and then removed from the site after consultation with the Office of the Bishop and/or police.
6. Inappropriate material that does not raise suspicion that a child has been or will be abused/neglected/exploited should immediately be removed from the site.
7. Any content that details inappropriate behavior (outside of the bounds of the established behavioral covenant) during a church sponsored event or activity should be addressed by adult youth leaders and parents.
8. Social networking groups for youth should be open to parents of current members.
9. Parents should be informed that the content of youth organization pages or groups that are not sponsored by the church are NOT within the purview of adult youth leaders.
10. Adult leaders of youth groups and former youth members who, due to departure, removal from position, or are no longer eligible because they "aged-out" of a program should be immediately removed from digital communication with youth groups via social networking sites, list serves, etc.

Recommended Practices and Guidelines for Interactions with Adults:
Social Networking Sites-Relationship

1. Clergy are strongly encouraged to set very stringent privacy settings on any social networking profile to shield both adult and youth members from viewing personal content that may be inappropriate.
2. Individual personal profiles of clergy are to be used to interact with real friends, family and peers. Clergy should not submit "friend" requests to parishioners and others to whom they minister. The disparity of power may not give the other person the ability to decline such request.
3. Clergy who want to connect via a social networking website with parishioners are strongly encouraged to set up an official Organization Page that all parishioners may join. The purpose of having a personal profile and an Official Organization page is to create a line of privacy and maintain healthy boundaries with parishioners and real family, friends and colleagues.
4. The Diocese of Milwaukee recommends official organization pages for parishes rather than group pages, which are unofficial and have limited tools for both privacy/security and outreach.
5. Clergy should consider the impact of declining a "friend" request from parishioners. These encounters may create a tension in "real world" relationships. Clergy can direct "friend" requests from parishioners to the parish's official organization page.
6. Clergy who work directly with youth are encouraged to establish separate church sponsored digital communications groups/pages for youth, to maintain contact with youth members.
7. When a cleric's ministry at a parish or other ministry setting ends, the cleric should remove parishioners as "friends" or contacts in all forms of digital communications.

Recommendations for digital communications and content Behavioral Covenants

1. Covenants should acknowledge that materials posted on Church Sponsored sites (and/or group pages) are NOT CONFIDENTIAL.
2. Covenants should acknowledge that content deemed inappropriate will be removed from the site or group page.
3. Covenants for communities of faith should address the following issues:

a. Appropriate language
b. Eligibility of membership to join a closed social networking group
c. Things to consider include whether to allow those who are not yet members of a parish or youth group to join, and whether there are age requirements/restrictions for participation for youth groups
d. Loss of eligibility of membership and removal from the social networking group
e. Consider how and when members will be removed from the group due to moving away, leaving the faith community, becoming too old for youth group, clergy leaving to minister to another parish or exclusion from ministry positions for other reasons
f. Who, how and when may photos be "tagged" (identified by name)? For example: individuals may tag themselves in photos but should not tag others. No one under the age of eighteen should be tagged by an unrelated adult.
g. Appropriate and inappropriate behavior of members (bullying, pictures that depict abuse, violence, sexual acts, etc.) and the consequence for inappropriate behavior
h. Compliance with mandated reporting laws regarding suspected abuse

Recommendations for Video Chats, Blogs or Video Blogs

1. Adults should refrain from initiating video chats with youth
2. Participants in a video chat or blog should consider what will be shown in the video such as their surroundings, their clothing/state of dress, etc.
3. All transcripts of on-line text chats, video chats, blogs or video blogs should be saved when possible.
4. All clergy and adults engaged in ministry with youth should consider the content and nature of any post that will be read by or visible to youth.
5. Your voice is often considered the voice of the church.

Recommendations for Publishing/Posting Content Online

1. Congregations must inform participants when they are being videoed because church buildings are not considered public space.
2. Any faith community that distributes video of its worship services or activities on the web or via other broadcast media MUST post signs that indicate the service will be broadcast.
3. All communities of faith should take care to secure signed Media Release forms from adults and guardians of minor children who will or may participate in activities that may be photographed or videoed for distribution.
4. Photos that are published on church sponsored sites should not include name or contact information for minor children or youth.

Recommendations for Use of Email or Texting (Includes Twitter)

1. Email can be an appropriate and effective means of communicating basic factual information such as the time of an event, agenda for a meeting, text of a document, etc.
2. Email is not an appropriate communication method for matters that are pastorally or legally sensitive, emotionally charged or require extensive conversation.
3. If an email message is longer than a couple of sentences, then the matter might more properly be addressed via live conversation.
4. Humor and sarcasm can be easily misinterpreted in an email.
5. All email users should take a moment to consider the ramifications of their message before clicking on the "send" or "reply to all" button.