Halifax United Methodist Church
Cyber Safety Policy

The internet and portable devices allow people to stay in contact with each other more easily than at any other time in the history of civilization. Some incredible ministry can take place using modern technology, but as with all forms of ministry there are some inherent risks involved with the use of electronic communications. However, following basic Safe Sanctuaries procedures can help to minimize those risks. There is no such thing as privacy in cyberspace. Consider anything and everything on the internet as public information. Here are some recommendations:

Receive Parental/Guardian Permission

In addition to general permission to participate in an HUMC ministry, it is advisable to receive advance parental permission for children and youth, and personal permission for vulnerable adults in writing for:

1. Posting photos of participants on any websites or sending them e-mail or cell phone messages or making videos for any use;
2. E-mailing, Instant Messaging (IM'ing), calling, texting, or sending data to a child, youth, or vulnerable adult by computer, PDA, or cell phone; and
3. The sharing of any full name or contact information.

Never Post Easily identifiable Information Online.

1. If you communicate by email, do not use "broadcast" emails. Use the "BCC" (blind carbon copy) so that each recipient sees only his or her address when a message is received.
2. Be cautious when transmitting easily identifiable information like event dates, times, locations, or participants.
3. Limit what is communicated in electronic prayer requests. When placing anyone on an electronic prayer list, consider using only first names.

Limit individual communications with children, youth, and vulnerable adults.

1. Conduct any communications in a professional manner. (Even though you may be a sounding board for a person having a bad day, the reverse is not true.)
2. Save all confidential cyber-communications you have with children, youth, and vulnerable adults (i.e., instant messages (IM's) chat room conversations, emails, etc.). An electronic paper trail can be important.
3. If you are uneasy about any topic addressed in an email or in an email in general, send a BCC to a parent/guardian (if appropriate) or another trusted adult. Honor privacy, but not secrecy.
4. If abuse is divulged electronically, follow standard reporting procedures.

Safety Measures for Sharing Photos Electronically

1. Obtain permission to use photos.
2. When posting photos, refrain from using names and never use last names or identifiable information.
3. Check photos for vulnerable/compromising situations and make sure they uphold your mission.
4. Block "save photo as" options on websites (ask a web savvy person for assistance).
5. Limit access to photos by employing the use of a password.

Safety Measures for Using Social Networking Sites

Social networking sites such as MySpace, Facebook, 7Villages, Xanga, Friendster, Plaxo, and others are popular with many people:

1. Set privacy settings to limit who can see your profile, otherwise people may still be able to view your full profile.
2. Restrict who can be your friend. It is prudent to use judgment in accepting requests from youth.
3. Use higher level security features even if you have a restricted profile (such as requiring your approval of all comments posted to your site.)
4. Do not post anything to your social networking site that you would not want attached to your resume or printed in the church bulletin or newsletter (the same goes for blogs).
5. Remove or do not post inappropriate comments, photos, etc.
6. Encourage youth to follow these same guidelines.