DIOCESE OF FORT WAYNE – SOUTH BEND

Policy and Standards

Use of computers, internet and electronic communication

Including faxing

by all

employees, volunteers and students

July 2013

DIOCESE OF FORT WAYNE – SOUTH BEND

Policy and Standards - - Use of computers, internet and electronic communication including faxing by all employees, volunteers and students

The Diocese of Fort Wayne – South Bend may supply computers, internet access, and other electronic communication devices to its employees, volunteers, or students in order for them to complete the responsibilities assigned by their positions. The diocese believes these resources are an important educational and evangelizing tool to further the mission of the Church. Therefore, use of these resources must always be consistent with the mission of the Catholic Church. Employees, volunteers, and students must take care to use these tools for their intended purposes. The diocese may monitor user accounts, internet activity, email communications, or any other related use of computers and its networks at any time, with or without notice to users.

Computer use

In using a computer supplied by the Diocese of Fort Wayne – South Bend or one of its entities, all employees, volunteers, and students must:

1. Respect the privacy of other users.
2. Respect and honor copyright and license agreements.
3. Safeguard their user identification (user ID) and private passwords.
4. Protect information from unauthorized use or disclosure.
5. Never use the computer for illegal purposes or in any way that violates any international, federal, state or local laws.
6. Never use the computer to harass, threaten, or transmit inappropriate material.
7. Use diocesan computers for personal communication or work in very limited instances. Brief and occasional use is acceptable as long as it is not excessive or inappropriate, occurs only on personal time, and does not interfere with a person's work. Incidental and occasional personal use of electronic mail is permitted. Such messages should comply with this Policy and Standards and may be monitored.
8. Never use diocesan computers for personal purchases.
9. Never send, trade or store personal photos, videos, music or other items on the network as this greatly impedes system back-up.
10. Use computers and the networks to which they are linked conscientiously so as not to drain or monopolize the system such that the work of others is impeded. If a person is unsure about the impact of their use, they should contact the Diocesan Business Office.
11. Never delete any computer files or download diocesan information without appropriate authorization when separating from employment or volunteer service with the diocese.
12. Run frequent scans of computers for viruses and other malware. Any problems should be reported to the Diocesan Business Office. The use of USB Devices and Portable Storage Media has become more widespread. These devices present a security risk because they might carry viruses or expose sensitive data if they are lost or stolen. All USB devices and portable storage media including cell phones, IPOD's, memory sticks, and CD's may not be connected to any Diocesan laptop,

desktop or any other computer without the express written approval of the employee's supervisor.

13. Not use programs obtained from bulletin boards, home, friends, or other unauthorized sources on any diocesan equipment.

Websites/internet access

In accessing and using the internet, all employees, volunteers, and students must adhere to the above mentioned items. Also they must:

1. Never access, post or send immoral, obscene, illegal, threatening, abusive, defamatory, or profane material or pornography (adult or child) of any kind.
2. Never attempt to block, bypass or remove filtering software.
3. Use the internet for personal communication or work only in very limited instances. Brief and occasional use is acceptable as long as it is not excessive or inappropriate, occurs only on personal time, and does not interfere with a person's work.
4. Never use the internet for personal purchases.
5. Use great care when downloading files from the internet to the diocesan system. Files must be scanned for viruses. Compressed files should be scanned before and after decompression.

Electronic communication

In using electronic devices to communicate, including but not limited to email messages, text messages, tweets, websites, blogs, and social networking sites, employees, volunteers, and students will:

1. Always use respectful language.
2. Maintain appropriate relational boundaries in all forms of communication.
3. Never access, post or send immoral, obscene, illegal, threatening, abusive, defamatory, or profane material or pornography (adult or child) of any kind to any person.
4. Never send anonymous messages.
5. Send personal communication only in very limited instances. Remember, all communications may be monitored. Brief and occasional messages may be sent as long as it is not excessive or inappropriate, occurs only on personal time or in emergencies, and does not interfere with a person's work. Neither should an employee use his or her own personal communication device during work time.
6. Treat all communication as if it were public. Communication via these forms of technology does not always remain private. It is like sending a postcard. Many people can and will read it. Some might even change it. Always use language and communicate as if you were face to face with the person.

For adults, when communicating with children or young people

1. Remember you are an adult professional who is rendering service to a child/young person. You are not a friend or buddy.

2. Seek permission from parents before using email, text messages, or any other kind of electronic means to communicate with youth.
3. Always copy parents on messages sent to youth.
4. Never befriend children or youth when using social networking sites.
5. Never use a personal site on social networks to communicate about diocesan or parish events. Instead create and use a parish site or use the diocesan site for these purposes. Be sure you have your supervisor's permission before creating and using a parish or diocesan site, especially if children/young people will access it. If creating a special site, monitor it frequently for appropriate material and use. *Note: School personnel must abide also by all school policy on this issue.*
6. Never post photographs, personal information, or other identifying material about children/youth without the permission of their parents. Use great care before posting any information once permission is received.

Additional information for social networking sites (As part of a parish or diocesan site)

1. Site must adhere to the parish and diocesan policy on consent to use of pictures.
2. Site must be set to PRIVATE such that only authorized members can gain admittance and the public does not have access to the content.
3. A Youth Minister or Volunteer must not 'seek' friends but allow teens to request him or her first.
4. A Youth Minister must approve each request for membership after verification of current participation or leadership in the youth program.
5. Password must be difficult and frequently changed to avoid unauthorized access.
6. Application/features and all communications must reflect Catholic values.
7. Absolutely no tagging pictures with the youth names or other identifiers which could show up in search engines can be used.
8. On the request of a parent or legal guardian, the site must be made temporarily accessible for review of content.
9. Post rules of conduct on the site.

Revised July 2013
Promulgated by Most Reverend Kevin C. Rhoades on October 18, 2013