SECTION ELEVEN: USE OF TECHNOLOGY

This policy outlines acceptable use of both entity-owned hardware and software as well as personal technology and systems used for work.

A. Computers, Tablets, Smart Phones, E-Mail, Voice Mail, Internet

A.1 Employees use both entity-provided equipment and personal equipment connected with the entity and/or its network on a regular or intermittent basis.

A.2 Employer-provided equipment, e-mail and voice mail systems, and internet access accounts are the entity's property. Information temporarily or permanently stored, transmitted or received on these devices and systems (including personal password-protected web-based e-mail) and internet remains solely and exclusively the entity's property. Employees should not expect privacy when using these systems. Messages composed, sent or received, including attachments, are and remain the entity's property, and are not the employee's private property, regardless of the intended recipient.

A.3 Only an employee's diocesan email or the parish/school domain email is acceptable in the course of one's job. Personal e-mail addresses may not be used for the entity's business. Additionally, employees may not use diocesan or parish/school domain email to conduct personal business.

A.4 Software installed on the entity's computers, and on personal computers used for entity business should not be used for unlawful or improper purposes. All data temporarily or permanently received, collected, downloaded, uploaded, copied and/or created on any computer used for the entity's business may be monitored and may not be copied or transmitted to any outside party or used for purposes not directly related to the entity's business.

A.5 Employees must always use electronic devices and systems consistent with diocesan polices, applicable laws and regulations, and not contrary to the Diocese's and the entity's best interests. The following list of prohibited conduct is provided so employees are aware of the full scope of actions that may violate this policy. Employees may not use these systems and devices to:

a) transmit, retrieve, download, or store inappropriate messages or images relating to race, religion, color, sex, sexual orientation, gender identity and gender expression, national origin, citizenship status, age, disability, or other status protected by Federal, state and local laws
b) violate diocesan policies on safe environment, sexual misconduct with a minor, unlawful harassment and discrimination, and sexual harassment
c) make threatening or harassing statements to another employee, vendor, customer, or any outside party
d) alter, transmit, copy, download or remove any proprietary, confidential, trade secret or other information belonging to the entity or any of its constituents
e) send, receive, alter, transmit, copy, upload, or download proprietary software, databases, copyrighted or otherwise legally protected information or other electronic files without proper and legally binding authorization
f) download, transmit, or retrieve messages from multi-network gateways, real-time data and conversation programs including, but not limited to, instant messaging services, internet chat rooms and bulletin boards during work hours, unless necessary for business purposes
g) use or allow another individual to use these systems for any purpose that damages or jeopardizes the Diocese's reputation and mission or is detrimental to its interests
h) violate or fail to comply with laws applicable to trademarks, copyrights, patents and licenses to software and other electronically available information
i) solicit personal business opportunities or conduct personal advertising
j) engage in gambling of any kind, monitoring sports scores, or playing electronic games

k) engage in day trading or purchase or sell stocks, bonds or other securities; transmit, retrieve, download or store messages or images related to the purchase or sale of stocks, bonds or other securities
l) violate diocesan social media, social networking and weblogs policy
m) violate the federal Anti-SPAM law
n) transmit unsolicited commercial electronic mail promoting the entity's services without prior authorization from the employee's supervisor
o) transmit unsolicited commercial electronic mail promoting the employee's personal business, goods, products and services
p) initiate transmission of a commercial e-mail message that contains or is accompanied by false or misleading information
q) use personal storage devices or copies of software or data in any form on any entity computer without both obtaining specific authorization from the appropriate manager and scanning the data for viruses
r) take unauthorized photographs or videos using any handheld device, whether Diocesan-owned or personal, on entity property
s) use devices to photograph, video record or otherwise record any **minor** for any reason unless prior written permission has be granted by the minor's parent or legal guardian.

A.6 As legally permitted, the entity's monitoring may include physically inspecting hard drives, memory devices, and handheld devices. The entity retains the right to review content passing through its network, data lines, and other systems, personal e-mail (including personal web-based password-protected e-mail) and text messages accessed using the entity's computers and/or communication connections; key loggers and other input monitoring mechanisms; screen monitoring software, hardware, and video drives or other monitoring methods.

A.7 Knowingly and repeatedly introducing viruses into the entity's systems through improper use is subject to corrective action. Employee-caused damage to the entity's computer system through its unauthorized use may be charged to the employee.

B. Handheld Devices and Driving

B.1 Operating a motor vehicle while using handheld devices in performing job duties, including talking, e-mailing, texting and instant messaging is prohibited. Employees must stop their vehicle before using their handheld device. If it is necessary to communicate while driving, employees must use the hands-free device in a manner which does not impair driving ability. Traffic violations resulting from using handheld devices are the employee's sole responsibility. Because misuse of handheld electronic devices is a potential safety hazard, under no circumstances are employees required to, or allowed to, place themselves or others at risk to fulfill job requirements.

C. Social Media, Social Networking and Weblogs

C.1 The Diocese uses social media as a valuable tool for business and ministry missions, and employees may be required to use these platforms as part of their job responsibilities.

C.2 Employees must exercise sound and moral judgment when using social media, social networking sites, and blogs. Work-related social media activity should be respectful of the Catholic Church, supervisors, colleagues, and the people the Diocese serves. Employees must not post material that is obscene, vulgar, defamatory, threatening, discriminatory, harassing, abusive, hateful, or embarrassing to another person or entity, or that reflects negatively on the Catholic Church, the Diocese, its affiliates, employees, parishioner's, clients, students, volunteers and others we serve. Using social media at any time is public behavior that calls for at least as much discretionary judgment as one's personal public conduct.

C.3 Employees may not:

a) list their employee e-mail address or employer-issued phone numbers unless the social media, social networking site or blog is used solely for diocesan, parish, school, or Chancery business and has been authorized by the employee's senior manager (i.e. pastor, principal, administrator or department director)
b) post a picture or likeness of a student, parishioner, volunteer, co-worker, manager, supervisor, client or vendor without that individual's express advance permission
c) access sexually-based or discrimination-based websites
d) engage in any on-line activity that reflects or may reflect negatively on the Catholic Church, the Diocese, its affiliates, employees, parishioners, students, clients, volunteers and others we serve

C.4 Employees should have no expectation of privacy while using social media, the networks, and internet programs while at work or on the entity's equipment. Information created, transmitted, downloaded, exchanged or discussed may be accessed by the entity any time without prior notice. Employees are personally responsible for the commentary they express and the material they post while engaging in online social networking and blogging activities.

C.5 Violations of the Use of Technology policy are subject to corrective action.