DIOCESE
OF
ORLANDO

Teaching and Living the Light of Christ

Diocese of Orlando

DIOCESAN EDUCATIONAL TECHNOLOGY PLAN

Office of Catholic Schools
50 East Robinson St.
Orlando, FL 32801

Approved by: Secretary for Education / Superintendent of Catholic Schools

July 1, 2023- June 30, 2026

Table of Contents

Mission

Catholic schools in the Diocese of Orlando proclaim the Gospel message within an academic environment of excellence. We challenge students to be creative and critical thinkers who integrate faith, worship, moral leadership and compassion in order to create a more just and humane world. Technology in the Diocese of Orlando will support, enhance and optimize the learning process for all students in all Catholic schools. Emerging technologies will influence the formation of foundational skills in students to aid them in reaching their potential in a constantly changing world. Technology must be implemented seamlessly, as everyday experiences and must promote higher student achievement and a deeper understanding of their Catholic faith.

Vision

Technology will be used to enable learning and to integrate Diocesan curriculum. The curriculum and data must be the driving force for choosing any technology at the school both hardware and software.

The following objectives for a vision are encouraged at each school location in the Diocese of Orlando:

- To use technology to increase exposure to and foster understanding of other cultural, political and geographic areas, resulting in students becoming part of the global community and proclaiming the Gospel message
- To provide safe access to state-of-the-art technology/technological development for use with all students, educators, staff, and parents
- To use current and emerging technologies to enhance educational and faith opportunities for all students, educators, staff, and parents
- To provide technology-based educational opportunities for all educators, staff members, and parents
- To encourage educational use of technology that students may have at home and provide parent education on online safety best practices and digital citizenship
- To develop individual school technology plans derived from the Diocesan Educational Technology Plan and to follow Diocesan Cybersecurity Plan
- To implement a method to annually review the technological and cybersecurity needs, including equipment and programs, at school sites throughout the Diocese and compare with other schools within the state and nation.

General Introduction/Background

District Profile

The Dioceses of Orlando was established on June 18, 1968. In 1968, there were 50 parishes with 128,000 Catholics. Prior to this, the Diocese of Orlando was part of the Diocese of St. Augustine and during this time, 30 out of our 35 schools were built. Today the Diocese of Orlando has 80 parishes and 11 missions that serve more than 800,000 Catholics. The Diocese currently encompasses 11,254 square miles in nine counties: Orange, Seminole, Lake, Brevard, Osceola, Volusia, Polk, Sumter, and Marion County. The Office of Catholic Schools oversees 40 schools – 30 elementary schools, five high schools, one special education school, and four early learning centers, serving close to 15,000 students in grades Pre-K to 12. OCS supports approximately 1,200 educators, administrators and staff employed in the schools. The Central Florida area is surrounded with technology rich organizations with the Hi-Tech Corridor, Space Coast, University of Central Florida, Central Florida Research Park, and the Medical City in Lake Nona therefore the community expects that our schools be on the cutting edge of technology.

Location of Elementary and High Schools in the Diocese of Orlando

	Elementary Schools	High Schools	Total
Urban	17	3	20
Inner City	0	0	0
Suburban	15	2	17
Rural	3	0	3
Total	35	5	40

Elementary Schools PK-8 Enrollment by Race 2022-2023

	CATHOLIC	NON-CATHOLIC	UNKNOWN	Total
Amer. Indian/Native Alaskan.	17	3	0	20
Asian	356	76	5	437
Black/African American	376	447	15	838
Native Hawaii /Pac. Isl.	26	9	8	43
White	6959	1208	131	8298
Two or More Races	867	211	15	1093
Unknown	104	12	11	127
TOTAL	8707	1966	185	10856

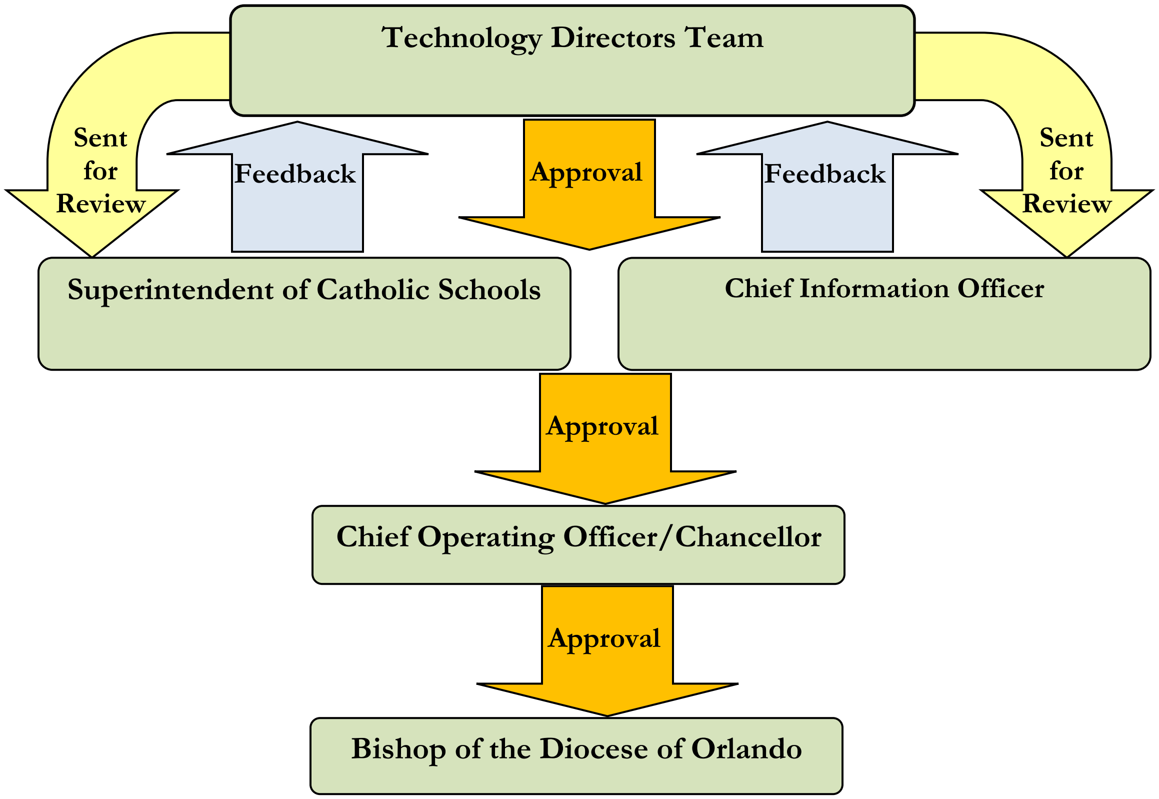
High Schools Enrollment by Race 2022-2023

	CATHOLIC	NON-CATHOLIC	UNKNOWN	
Amer. Indian/Native Alaskan	4	2	0	6
Asian	129	22	1	152
Black/African American	105	95	0	200
Native Hawaii /Pac. Isl	2	0	0	2
White	1741	391	0	2132
Two or More Races	587	69	0	656
Unknown	26	16	3	45
TOTAL	2594	595	4	3193

Planning Process

During the spring of 2020, the impact of COVID-19, closure of schools, and moving to fully virtual instruction presented our schools with many obstacles and demonstrated a lack of technology tools and training for our educators. Fortunately, our schools received assistance to purchase student devices, upgrade network infrastructure, and provide professional development to our educators. Our schools were able to turn difficulties into opportunities and for the next school year offered hybrid instruction, have achieved 1:1 in all grades, and educators have adapted to use digital resources. A team of school technology directors and the director of instructional technology at the Diocese of Orlando looked at the key categories of a Future Ready School; Curriculum, Instruction and Assessment, Use of Space and Time, Technology, Networks, and Hardware, Data and Privacy, Professional Learning, and Budget and Resources. Using these key categories and the newly released National Technology Plan, they began the process of updating the Diocesan Educational Technology Plan.

The approval process for the technology plan includes review and acceptance by the following groups:


Technology Directors Team
Sent for Review
Feedback
Approval
Feedback
Sent for Review
Superintendent of Catholic Schools
Chief Information Officer
Approval
Chief Operating Officer/Chancellor
Approval
Bishop of the Diocese of Orlando

Technology Directors Team	
Margie Aguilar	Office of Catholic Schools, Director of Instructional Technology
Julio Irizarry	Bishop Moore Catholic High School, IT Director
Lisa Jones	Annunciation Catholic Academy, IT Director
Jen Jones	Resurrection Catholic School, STREAM Coordinator
Brandon McCurry	St. Paul Catholic School, Technology Teacher
Stacey Miller	St. Thomas Aquinas Catholic School, IT Director
Sandy Neal	St. Joseph Catholic School, Technology Integration Specialist
Colton Singletary	Consultant, ColTech
Carl Sterling	Consultant, Sterling Technologies
Tony Vargas	Our Lady of Lourdes Catholic School, IT Director

Diocese of Orlando	
Most Reverend John Noonan	Bishop of the Diocese of Orlando
Ms. Theresa Simon	Chief Operating Officer/Chancellor
Mr. Henry Fortier	Secretary for Education / Superintendent of Catholic Schools
Mr. Jack Paige	Chief Information Officer

Needs Assessment/Goals

The Diocese of Orlando, Office of Catholic Schools utilized the standards and benchmarks from the National Standards and Benchmarks for Effective Catholic Elementary and Secondary Schools (NSBECESS), the goals on the National Education Technology Plan, and the International Society for Technology in Education's National Standards to develop its own list of needs and goals. Using as guide the National Educational Technology Plan from the Office of Educational Technology, the planning team divided the goals into five key areas: Learning, Teaching, Leadership, Assessment, and Infrastructure. Each school will develop a technology plan based on the goals established in the Diocesan Educational Technology Plan.

Goal 1: Learning: Engaging and Empowering Learning Through Technology

All students will have engaging and empowering learning experiences in both formal and informal settings that prepare them to be active, creative, knowledgeable, and ethical participants in our globally connected society. (NSBECESS 2.1, 2.4, 3.2, 7.3, 7.4, 7.6)

Objective 1.1: Design collaborative classrooms through the use of technology, room design, and provide digital devices to each student.

Objective 1.2: Focus on modular solutions that can be adapted to changing educational needs and environments.

Objective 1.3: Facilitate opportunities in the instruction for students to engage in multimedia creation, blended learning, and personalized learning.

Objective 1.4: Empower students to not only draw upon information from multiple sources but also to evaluate the validity and accuracy of the information.

Objective 1.5: Implement the use of global communication technologies to allow for online collaboration and global awareness, monitored by the teacher. Examples are: Student email accounts, cloud storage, learning management system, audio/video broadcast, social media or backchannels, online collaboration, electronic portfolios, and others.

Objective 1.6: Establish an age appropriate internet safety curriculum and inform students of proper and ethical technology use under the lens of our Catholic faith.

Goal 2: Instruction: Teaching with Technology

Goal: Educators will be supported by technology that connects them to people, data, content, resources, expertise, and learning experiences that can empower and inspire them to provide more effective teaching for all learners. (NSBECESS 7.4, 7.6, 7.7, 7.9, 7.10, 8.1, 8.3)

Objective 2.1: Provide opportunities for educators to have access to cloud-based content, resources, and tools such as interactive technologies and digital learning devices for all students.

Objective 2.2: Enable a classroom management tool for educators to control student devices in order to personalize learning and create experiences that are more engaging and relevant.

Objective 2.3: Organize learning around real-world challenges and project-based learning using a wide variety of digital learning devices and resources to show competency with complex concepts and content applying ISTE Standards for Students.

Objective 2.4: Develop videos/screen captures for educators with steps on how to use software, equipment, and how to do maintenance and simple troubleshooting.

Objective 2.5: Provide educators with professional learning experiences powered by technology to increase their digital literacy and enable them to create compelling learning activities that improve learning and teaching, assessment, and instructional practices.

Objective 2.6: Establish and maintain an information security awareness program for educators on cybersecurity, internet safety, reporting potential attacks, and personal confidential information using the lens of our Catholic faith.

Goal 3: Leadership: Creating a Culture and Conditions for Innovation and Change

Goal: Embed an understanding of technology-enabled education within the roles and responsibilities of education leaders at all levels, and set diocesan and local visions for technology in learning. (NSBECESS 6.5, 7.1, 8.1, 10.4, 12.3)

Objective 3.1: Expand the use of parent/student SIS (student information system) portal for communication, data collection, online registration and enrollment to streamline and reduce cost of operations and effectively communicate with all stakeholders.

Objective 3.2: Utilize an issue tracking application to manage and monitor IT and maintenance requests and rethink the roles and responsibilities of existing staff members to support technology in learning.

Objective 3.3: Set technology competency expectations for all educators and establish technology as integral to most learning designs, used daily within and beyond the classroom.

Objective 3.4: Include in school budget a line item for annual technology as well as in capital expenses for maintenance and replacement (devices, network, and tools) to ensure technology remains up-to-date and long-term sustainability.
Objective 3.5: Establish a school technology committee to provide guidance to the school leaders and develop a sustainable technology implementation plan.
Objective 3.6: Leverage community resources and local partnerships to support high-quality academic and enrichment opportunities for educators and students.

Goal 4: Assessment: Measuring for Learning
Goal: At all levels, our Diocese and schools will leverage the power of technology to measure what matters and use assessment data to improve learning. (NSBECESS 8.1, 8.2, 8.3, 8.4, 8.5)
Objective 4.1: Implement methods of technology-based formative and summative assessments that provide educators with timely and actionable data and feedback in order to create personalized digital learning experiences.
Objective 4.2: Apply the use of assistive technology features on assessments in order for students to better demonstrate what they know and how to apply this knowledge.
Objective 4.3: Utilize adaptive assessments to facilitate differentiated learning and provide students with timely feedback.
Objective 4.4: Enable technology-based assessments that allow for a variety of question types such as graphic responses, simulations, equation responses, and performance based in order to demonstrate more complex thinking.
Objective 4.5: Employ learning dashboards to integrate data from assessments, learning tools, educator observations, and other sources to provide comprehensive graphic representations of student progress in real time and offer resources to help students continue their learning.

Goal 5: Infrastructure: Enabling Access and Effective Use
Goal: All students and educators will have access to a robust, comprehensive, and safe infrastructure when and where they need it for learning. (NSBECESS 12.1, 12.2, 12.3)
Objective 5.1: Improve the integrity, reliability, and speed of the schools' local area network (LAN) with a minimum one gigabit twelve strand fiber backbone and Wi-Fi access inside and outside classrooms.

Objective 5.2: Move to cloud servers when possible, if not possible maintain acceptable servers in well-ventilated secured room, and maintain and test a backup system.
Objective 5.3: Utilize a centralized endpoint detection and response system and content filter that screens and excludes from access or availability web pages deemed objectionable to students.
Objective 5.4: Implement a remote monitoring and management software for all the school devices, track and manage all hardware and software applications.
Objective 5.5: Provide access to managed mobile devices that connect learners and educators to the vast resources of the internet and facilitate communication and collaboration.
Objective 5.6: Follow the Diocesan Cybersecurity Plan and the Technology Responsible Use Policy to safeguard educators and students and ensure that the infrastructure is used to support learning.

Funding Plan

The Diocese of Orlando Office of Catholic Schools explores every source to obtain funds for technology in the schools. Funding sources for the improvement and acquisition of technology comes to the schools primarily through grant applications, fundraising, donations, capital funds, and general operating funds at the schools' site. The Office of Catholic Schools does not have funding to give to the schools to support technology endeavors that is why it is recommended that each school has a technology line item in their budget and the items listed under it are truly a technology need. Another source of funding is adding a Technology Fee per student to help offset the cost of maintaining and upgrading equipment. Also, the school should have a refresh plan for all equipment, which will enable budgeting and forecasting for future purchases. It is recommended to have four-year refresh plan for end user devices and seven-year plan for network equipment. Furthermore, the Catholic schools in the Diocese of Orlando are also expected to fully participate in their local education agencies' federal programs. Finally, the Diocese of Orlando, Office of Catholic Schools has created a consortium to apply for E-Rate for each of the schools. Participation in the E-Rate program is expected from all the schools via the consortium or independently filing for funding.

Technology Acquisition Plan

The Office of Catholic Schools negotiates Diocesan pricing and encourages schools to participate in Diocesan group purchases. Also, recommends implementing a single source vendor for school owned devices (Windows, Chrome, Apple). The schools need to take advantage of buying in volume by combining purchases or leasing from one single vendor. In addition, collaboration on some of the platforms that can be used across all entities in order to standardize and leverage our size when it comes to licensing/hosting, etc. The initiative of formalizing a uniform standard for hardware purchases ensures technology will enhance student achievement and comply with 21st Century in the most cost-effective manner.

The Office of Catholic Schools Director of Instructional Technology has created a guide of suggested hardware and software products. Also, a list of approved vendors with a history of reliable products and acceptable support and training is available to help schools when making purchases. The identification of appropriate technologies will be based on recommendations from the technology coordinators at the schools. Therefore, when schools are procuring technology hardware and software they must consult with the Director of Instructional Technology at the Office of Catholic Schools. In cases involving the combination of parish and school technology they must consult with the Chief Information Officer and Vice President of Financial Operations.

It is very important that the hardware is purchased with warranty to last the life of the product as a viable one. Once the warranty runs out, it should be placed as extra hardware and be replaced in case of failure. Considerations for software and hardware purchases are total cost of ownership, consistency, upward migration, manageability, maintenance, training and support.

Access

The Office of Catholic Schools has an overall goal of attaining equity among all schools of the Diocese of Orlando. OCS is aware that some schools have more resources to fund technology than others. To ensure student equity throughout the Diocese's schools, it is recommended pursuing alternate funding sources to bring state-of-the-art technology into every classroom.

Developing a refresh program to address device and network obsolescence will help establish the direction each school needs to go. Also, the need to retrofit some schools with up-to-date infrastructure will help to access other funding sources coming from the Diocese and E-Rate Category 2 Services. In addition, the refresh program will make available devices that are obsolete to the schools to be given to students without access to technology outside of their classroom.

Our students are more successful when parents are involved and informed. Therefore, equitable access to information and other technologies to support teaching and learning must be available on every school's portal. Examples of some of those programs are Britannica Online, Discovery Education, Sarah, BrainPOP, and Neptune Navigate.

The Diocese of Orlando has developed a Social Media Communication Policy that all administrators, educators, and staff have to sign in order to have access to all the systems including internet. This policy maintains the integrity of systems, programs, and information resources. It also protects the confidentiality of students and the intellectual property rights and licensing agreements. The Office of Catholic Schools has created a Technology Responsible Use Policy for all students. This policy is revised and updated every year, and both students and their parents have to sign in order to have access to all the network resources provided by the school. The schools have to monitor and filter internet access to all students utilizing software or hardware that blocks content that is obscene, harmful or pornographic to minors.

User Support Plan

The main goal for the user support plan is finding cost effective solutions and using existing resources to the fullest. Ideally, a Technology Specialist should be located at every school to provide onsite support. If this is not possible, the school should obtain contracted services to maintain the equipment. Some of the options that schools may use for support of technology are as follows:

1. Offer training at the beginning of the school year to educators in troubleshooting and provide them with a troubleshooting guide.
2. Create a Help Desk system where problems can be recorded, tracked, and queued in order of importance.
3. Create an Online Educator Resource Center with video tutorials, assistance, and education resources for educators and administrators.
4. Standardized the school's hardware including devices (Apple, Chrome, Windows), document cameras, interactive displays, and printers and obtain service and support.
5. Standardized the school's software, offer training, and provide user's guide.
6. Develop a group of students (Tech Team) that can help provide technology support through the school.

7. Utilize tools to develop collaboration between educators and forums to share and discuss ideas.
8. Provide staff, educators, and students with annual training on cybersecurity, online safety, and data privacy.

Staff Training Plan

To support the technology initiatives that are implemented within the Diocese, each school must survey educators needs at the beginning of the school year. From the needs assessment, it is essential to create a comprehensive professional development plan and submit the plan to the Office of Catholic Schools. The training is provided for instructional, administrative and non-instructional personnel and is offered in a variety of models like district workshops, guided modules, school-based training, and online training.

Online training modules can be developed on specific content areas that are computer based. These guided modules also support the effort to keep educators to remain in the classroom in lieu of workshops during the school day. School based training can be conducted by the school technology coordinator or by the Diocesan Director of Instructional Technology at the school site on a specific topic. Finally, attendance at conferences like FETC and ISTE are encouraged and the Office of Catholic Schools provides training opportunities for all Technology Directors.

Program Evaluation Plan

The Diocese of Orlando Office of Catholic Schools uses three instruments to evaluate the program and make the necessary adjustments. First, the Professional Development Committee prepares an annual online survey for educators. This survey is tabulated and the Committee can prepare a plan for professional development providing training on the identified areas. Next, a Technology Data Sheet is prepared by each school that documents an inventory of hardware and software in the school and identifies concerns and immediate goals for the site. This Data Sheet is reviewed by the Director of Instructional Technology and recommendations are made for improvement. Lastly, the Office of Catholic Schools has arranged to use Florida Innovate Tools to identify areas in which educators and administrators need training and assess proficiency in students.

Appendix A:
Social Communications Policy

Social Communications

Social Communications deals with the all the problems raised by the cinema, radio, television, the daily and periodical press, and digital media in relation to the
interests of the Catholic religion.

Standards for All Social Communications Policies

1.0 Glossary of Terms

1.1 "Administrator": The person who creates a social media site, be it public or group. An administrator also posts information (e.g. text, video, audio, images); screens comments; and manages the activity. Each social media site should have no more than four administrators and at least one must be an employee of the Diocese of Orlando who is a director at the Chancery or parish level (or equivalent) and must have written permission
of pastor or immediate supervisor.

1.2 "Church Personnel": For purposes of this policy only, Church Personnel includes all individuals who minister, work, or volunteer in any school, parish, or ministry of the Diocese whose compliance with this policy is sought. The term has no legal meaning or significance outside the scope of this policy and is not indicative of any employment or agency relationship.

1.3 "Consultant": Independent contractors, consultants, vendors or other persons who are not subject to the supervision of the Bishop of the Diocese and for whom no such duty to withhold payroll taxes exists, but provide expertise on database creation and/or management, IT services, or internet-related services.

1.4 Diocesan entity: Any parish, school, entity or ministry of the Diocese of Orlando, including those entities which are separately incorporated under 501 (c) (3).

1.5 Domain: The unique internet registered address of the entity. The Domain should be registered in the name of the entity and used for all official business and email.

1.6 "Employee": Any lay person who is employed by any Diocesan entity, whether part- time or full-time, who is given payment for services rendered, and for whom the Diocesan entity is obligated to withhold payroll taxes (FICA, Medicare, and withholding).

1.7 Group Social Media Site: This site is also known as a list serve or discussion forum. A group site can only be viewed by invitation or request. The administrator knows the people who are members and the members can interact. In Facebook, groups can be open, closed, or secret. The members and content of an open group are public. In a closed group, the list of members is public, but the content is private. In a secret group, the members and content are private, and the group doesn't appear in search results for non-members.

1.8 Internet: Includes both external and internal access of communications and data storage equipment, either owned or reserved for use by the Diocese, by digital information devices including personal computers (PCs), personal digital assistants (PDAs) and similar devices. The term "Internet," as it applies to external resources, is meant to be all-inclusive and comprises other similar or analogous terms such as the "world wide web," "e-mail," and "the Net."

1.9 Internet/Intranet/Extranet-related systems: include, but are not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, www browsing and FTP.
All internet/intranet/extranet-related systems are the property of the Diocesan entity it serves. These systems are to be used for business purposes in serving the interests of the Diocesan entity, its staff, and its constituents in the course of its normal operations.

1. 10 IT: Information Technology

1.11 Network: Communications system connecting two or more computers and their peripheral devices to exchange information and share resources.

1.12 Personal Social Media Site: Personal social media sites are created by an individual to stay connected with family and friends, and to interact with the online community—not for the purpose of ministry.

1.13 Public Social Media Site: A site that an administrator creates for public viewing. It is open to anyone who has internet access and therefore the administrator does not know the identity of the people who view or interact with the site.

1.14 Social Media Site: Any online technology that allows individuals to interact on some level to share information, dialogue or stay digitally connected. This includes many well-known sites for video sharing such as YouTube, social networking such as Facebook and microblogging such as Twitter. This policy does not list the approved social media sites because it is only intended to provide guidelines which should be applied to the digital media landscape which is ever changing. Social media includes web-based and mobile based technologies which are used to turn communication into interactive dialogue among organizations, communities, and individuals. Andreas Kaplan and Michael Haenlein define social media as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user- generated content."[1] Social media is ubiquitously accessible, and enabled by scalable communication techniques.

1.15 Spam: Unauthorized and/or unsolicited electronic mass mailings.

1.16 "Volunteer": Any unpaid person engaged or involved in a Diocesan activity, specifically as it relates to database creation and/or management, IT services, or internet- related services.

2.0 Scope

These policies apply to authorized users of any school, parish, or ministry of the Diocese of Orlando, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the Diocesan entity.

3.0 General Standards

3.1 Links

All Diocesan parishes, schools, and entities must have a link for the Diocese of Orlando website, www.orlandodiocese.org, and may have links to other Diocesan entities, such as San Pedro Center, www.sanpedrocenter.org; Catholic Charities of Central Florida,
www.cflcc.org; and Bishop Grady Villas, www.bishopgradyvillas.org on its own website. Any other links should not be in conflict with the teaching and the Magisterium of the

Roman Catholic Church. Acceptable links fall into these three main areas:

1. Official Church sites, such as the Vatican, U.S. Conference of Catholic Bishops, state conferences, archdioceses and dioceses;
2. Parts of the Diocese such as parishes, schools and ministries operated by the Diocese or approved resources associates with those ministries; and
3. Those under the oversight of a bishop or religious congregation, or listed in the Official Catholic Directory. Church leaders should use prudence in evaluating links to other commercial opportunities on its site. It is the entity's responsibility to evaluate its hosts' advertisers and sponsors on a regular basis.

3.2 Photos

Photos and video of an event may be posted on a social media site. Tagging of photos to identify the person(s) in the photo is not allowed. The Diocese Network Acceptable Use Policy should be followed with regards to photos/video/media.

1. Use of photos on websites should be group photos. Where children are involved, no names or first names only should be used. Parents/guardians must sign permission slips each year for use of children's photos; therefore, all photos, particularly those which include children, should be refreshed regularly.
2. Recording/Photography by Family/Friends: A parish/school/entity of the Diocese cannot be held responsible for recorded materials (e.g. audio, still and/or video) transmitted or placed without its knowledge or permission through electronic or other means or in external media of any type. For its official, sanctioned electronic resources, a parish/school/entity of the Diocese of Orlando has established acceptable use standards for recorded materials. It is suggested that parents and guardians follow these standards in their personal activities and on their Personal Social Media Sites. As such, parents, guardians, family members and friends who photograph or otherwise record school events should respect the privacy of others and should not identify another child by more than a first name in any transmission (e.g. mail, e-mail or internet website), unless authorized by the parent or guardian of that child.
3. Parents/guardians must sign permission slips each year for the use of video where children are present. Use of videos on websites should be refreshed regularly when images of children are present.

3.3 Catholic Identity

Information posted using any form of technology in the name of the Church must adhere to the following guidelines:

a. Content or information should be appropriate and affirm the teachings of the Catholic Church and its Magisterium.
b. Must be professional, respectful and courteous.

c. Must avoid debate of Catholic Church teaching.
d. Have the pastor (or supervisor) monitor content on a regular basis.
e. Only logos or photographs of ministries/organizations/vendors directly tied to the Catholic Church /or an approved site may be displayed on the page.
f. There shall be no offensive or disruptive messages, initiated either by the administrator or user. Among those which are considered offensive include, but are not limited to, messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment which offensively addresses someone's age, sexual orientation, belief system, national origin, or disability.

3.4 Transparency

1. It is essential to the nature of ministry that parents/guardians are fully aware of all mediums being used to keep in contact with their young person for ministerial purposes.
2. The intent of any communication policy is to give witness to the Good News to create a safe environment for all vulnerable populations, which is open, transparent and involves the parents/guardians of the young people as partners.
3. It is important that ministry is not used to establish private one-on-one relationships between adults and youth and our methods of communication must reflect this.
   - Adults must maintain copies of communication with youth (under 18) and copy parents on all e-mails and other electronic correspondence.
   - Adults must copy supervisor on individual correspondence with young adults (over 18) who have not completed high school.
   - Adults should copy supervisor on individual correspondence with young adults who have completed high school.
4. Unusual circumstances of a pastoral nature should be documented and shared with the pastor or one's supervisor as soon as feasible. The documentation of any such circumstance should involve a copy of any applicable communication from all types of communication medium.
5. The administrator's log on credentials must be shared with the pastor or appropriate supervisor. In addition, the administrator must provide credentials on any account on which the administrator has privileges.
6. Leaders of ministry must say "no" if asked to be a friend on a social media page of a youth (under 18) and should say "no" to parents, parishioners or other individuals who interact with them only through this leadership role. There are risks with social communications, especially with blurring boundaries of professional and personal relationships. Anyone can say "no" to someone who wants to be their friend. Ultimately, what employees do on their own time is governed by the Diocesan conduct policy.

4. Enforcement

Effective security is a team effort involving the participation and support of every authorized user who is using social communications. It is the responsibility of every authorized user to know these guidelines, and to conduct their activities accordingly. The Diocese of Orlando does not sanction any use of social communications that is not authorized by or conducted strictly in compliance with this policy and its regulations. Authorized users who disregard these policies may be subject to a change in their relationship with the Diocese, up to and including termination or removal from their volunteer position. In addition, any Employee found to have violated this policy may be subject to disciplinary action, up to and including termination. Administrators who have read and signed the Agreement and who agree to act in a considerate and responsible manner will be authorized users.

These rules are in place to protect authorized users and Diocesan entities. Inappropriate use exposes Diocesan entities to risks and legal issues. Anyone with knowledge of inappropriate use of social communications that is in violation of this or any other Diocesan policy should report this information verbally and in writing to the individual's supervisor.

4.1 Disciplinary or Legal Action

Failure to abide by this policy may result in disciplinary or legal action by the Diocese of Orlando. It is the responsibility of each entity (parish, school, other entity) to monitor the social media sites created by staff and ministry leaders.

Social Media Policy

1.0 Overview

Why Are Catholics Called to Use Social Media?

Social media is a fast growing form of communication in the United States among people of all ages. Our Church cannot ignore it, but instead engage social media in a manner that is safe, responsible and pastoral.

"…the new communications technologies must be placed at the service of the integral good of the individual and of the whole of humanity. If used wisely, they can contribute to the satisfaction of the desire for meaning, truth and unity which remain the most profound aspirations of each human being." Pope Benedict XVI, World Communications Day Message, June 5, 2011

Pope Benedict XVI also sends this note of caution: "Who is my "neighbor" in this new world? Does the danger exist that we may be less present to those whom we encounter in our everyday life? Is there is a risk of being more distracted because our attention is fragmented and absorbed in a world "other" than the one in which we live? Do we have time to reflect critically on our choices and to foster human relationships which are truly deep and lasting? It is important always to remember that virtual contact cannot and must not take the place of direct human contact with people at every level of our lives."

Social Media is to be utilized as a particular tool to continue the work of ministry, the purpose of which is to invite those whom we serve to become living disciples of Jesus Christ. It is essential that our ministries utilize the tools to that end, rather than being shaped by the technology itself.

Social media can only be one part of a multi-faceted approach to reach out to others and invite them to a life in Christ, in community, for the greater good of society. Information shared via a social network should also be available on a traditional website, one on one, in groups and via multiple channels of communication. This includes everything from personal conversations and phone calls, to the bulletin, flyers and mailings. The focus is evangelization, social media is simply one more tool, and not the end in itself.

- Social media is the online technology and methods that allow people to share content, personal opinions and insight with others. It implies a two-way communication between parties. It is not static. Content can come in many forms: text, images and photos, video, audio. It allows people to create a personal profile about yourself and then share and discuss with your circle of accepted friends and family. Example: Facebook
- Social bookmarks allow you to publicly share your list of favorite websites. Example: Delicious Online gaming allows users to interact with others for the purpose of an online game. Example: AdventureQuest
- Blogging allows people to write and publish their thoughts and opinions and have others provide instant feedback. Example: Wordpress
- Microblogging allows you to post in a short amount of characters information about your daily schedule or micro current event as it happens. Example: Twitter

Digital media is a form of electronic media where data are stored in digital (as opposed to analog) form. It can refer to the technical aspect of storage and transmission (e.g. hard disk drives or computer networking) of information or to the "end product", such as digital video, augmented reality, digital signage, or digital art. Florida's digital media industry association, Digital Media Alliance Florida, defines digital media as "the creative convergence of digital arts, science, technology and business for human expression, communication, social interaction and education". Digital Media does not imply two-way communication between parties.

- Wikis allow you to create, edit and share information about a topic. Example:

Wikipedia

- Video sharing allows you to upload and share video with others. Example: YouTube.
- Photo sharing allows you to upload photo and images that can be viewed by others. Example: Flickr and Pintrest
- News aggregator, also known as a feed aggregator, feed reader, news reader, RSS reader or simply aggregator, is software or a Web application which aggregates syndicated web content such as news headlines, blogs and podcasts in one location for easy viewing. Example Digg

2.0 Social Media Sites

2.1 Approval Process

You must request permission from your pastor, principal or appropriate supervisor about the formation of a social media site prior to its creation. If approval is granted, the administrator must sign a "Social Media Administrator Agreement" and the agreement should be filed with the appropriate supervisor.

2.2 Choosing an Administrator

In order to ensure content on a social media site is accurate and true to the Magisterium of the Catholic Church, it is important to have a web administrator that understands Catholic teachings and can communicate them effectively. It is also important to have at least two administrators and no more than four administrators for each social media site. At least one administrator must be a Diocese of Orlando employee who is a director at the Chancery or parish level (or equivalent). This will allow the responsibility of ensuring proper content is posted and monitoring of the site to be managed by the diocesan employee (director or equivalent) while up to three additional administrators are able to participate with adding content. The administrator log on credentials should be shared with the pastor or appropriate supervisor, as well as his/her own account with administrator privileges.

2.3 Administrative User Names and Passwords

Administrative account contacts for websites, email systems, discussion groups, social media accounts or any other service whether hosted internally or externally should be a senior manager of the organization who has responsibility over the Information Technology function. User name and password information for management of these services must be maintained by each entity in a safe and secure location. The location should be known only to the appropriate IT authority and a senior manager such as Pastor, Principal, Business Manager or CFO.

2.4 Professional Account for Ministry

Social media site accounts should be formed independently of a person's *Personal* Social Media account. The site must be created by a diocesan employee who is a director or equivalent with a *professional* account created for the purpose of ministry. The email address used for the establishment of the account must correspond with an entity email domain.

2.5 Comments

When possible, select the option to moderate comments before they are posted. There should be a comment policy on the social media site that explains what is allowed in terms of commenting. The public may comment on the administrator's posting as long as they follow the comment policy. An administrator should block anyone who violates the comment policy or displays any inappropriate conduct.

If there is an option to have comments or notification or alerts sent to your email, choose this so you will be aware of comments in a timely manner.

Comment monitoring means that you check your social media site on a regular basis and if someone has left a comment, you formulate a response and reply. If there is an inappropriate comment, you remove it and then you block the user (per your comment policy).

The Diocese of Orlando follows the comment policy of the United States Conference of Catholic Bishops.

The purpose of any a social media page is to provide an interactive forum where readers can gather and discuss information about the wide range of issues addressed by the work and mission of the Catholic Church, specifically through the Diocese of Orlando.

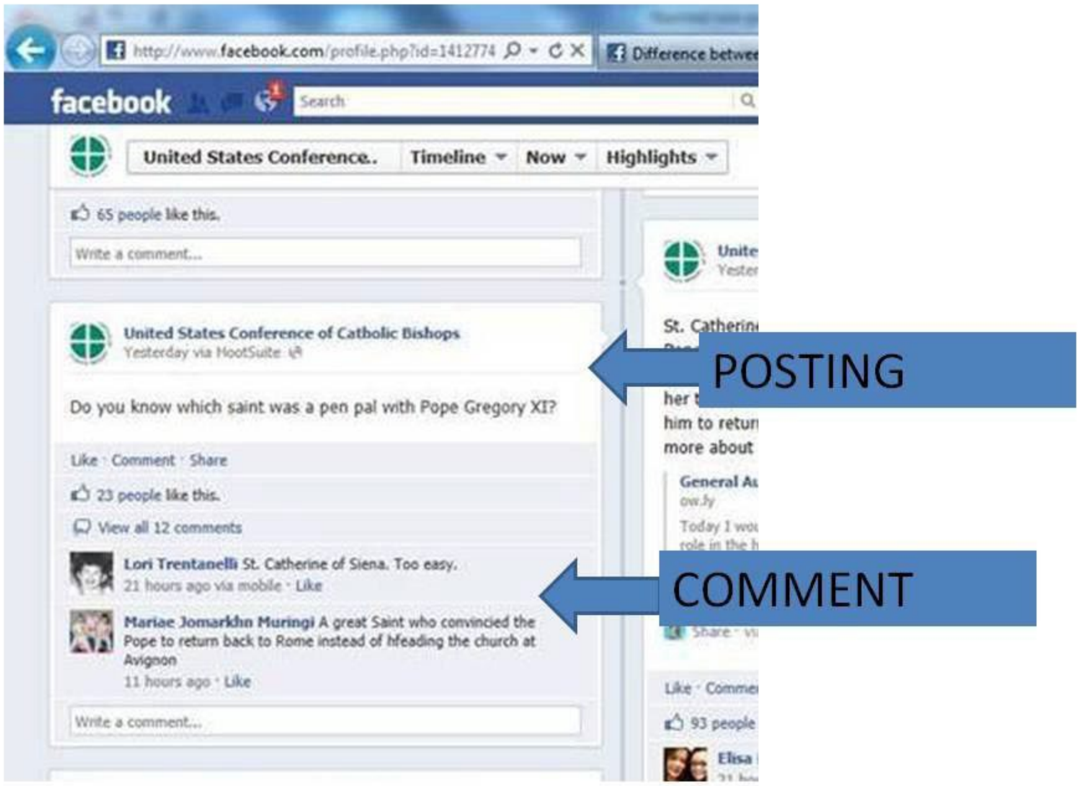
Followers are encouraged to post questions, comments and concerns, but should remember this is a moderated online discussion hosted by the Diocese of Orlando.

The Diocese of Orlando appreciates healthy, constructive debate and discussion; that means we ask that comments be kept civil in tone and reflect the charity and respect that marks Christian discourse. Comments that may be deleted include those that contain:

- Personal attacks/inflammatory remarks against a person or group
- Content/comments off topic
- Spam
- Links to sites that contain offensive material or attack the Church's hierarchy and its mission
- Promotion of services, products, political organizations/agendas
- Information that is factually incorrect
- Vulgar Language

The Diocese of Orlando reserves the right to remove posters who violate this policy. All sites must state that “Comments left by others on this page do not reflect the views of the Diocese of Orlando.”

2.5.1 The Difference Between a Posting and a Comment:



United States Conference of Catholic Bishops
Yesterday via HootSuite

Do you know which saint was a pen pal with Pope Gregory XI?

Lori Trentanelli St. Catherine of Siena. Too easy.
21 hours ago via mobile · Like

Mariae Jomarkhn Muringi A great Saint who convincied the Pope to return back to Rome instead of hfeading the church at Avignon
11 hours ago · Like

2.6 Fan/Follower/Member Photos

If the option exists to hide the fans, followers, etc. choose this. Otherwise, monitor the profile photos of your fans, followers, etc to remove anything that appears inappropriate.

2.7 Posting

Because our faith is alive and the content of your social media site should be ever changing, it is advised that you visit your site regularly for updates and to address any concerns within 24 hours or sooner if possible.

3.0 Instant Messaging

The Diocesan Networking Acceptable Use Policy does not allow the use of instant messaging on Diocesan networks or computer resources. Additionally, no instant messaging between youth and Ministry Leaders through a personal computer or other electronic device is permitted.

4.0 Age Restrictions

If there is an option to restrict access to a public social media site by age, the age limit should be defined as 13 and over. Minors under the age of 18 cannot join Facebook groups or other type of interactive opportunities unless total transparency and privacy is ensured. For those who are 18 years and younger (high school or elementary school students), Facebook "secret" groups are not allowed.

5.0 Advertising

Select to remove advertising when possible. Monitor the advertising and report anything inappropriate. Include a disclaimer on your social media site that you are not responsible for the content of the advertising and it is beyond your control.

6.0 Website Updating

A best practice is that information about an entity's events, activities and ministry appearing on a social media site is also reflected on the entity website so that the information is accessible in both areas. It is the administrator's responsibility to provide the content to the website manager at the same time that the information is posted to the social media site.

Unless serving in a dual role, the administrator is not responsible for how and when the website information is updated. If the administrator of the social media site is the website manager, this process can be more effective. If the website has an application that allows for simultaneous updating of social media sites and website, the process will be more effective.

7.0 Multiple Social Media Outlets for an Entity

There can be more than one social media site for each entity, if there is good reasoning for the use of multiple sites. No one should create a social media site in a vacuum. Pastors, principals, supervisors should be engaged in the conversation to determine its appropriateness and process. Planning ahead to determine the total need and coordination of branding and information sharing in real time is important in order for the sites to maintain their integrity and use. A qualified administrator who understands the nature of social media sites and the symbiotic relationship between them is important in planning for these sites.

8.0 Public Social Media Sites

Example of Public Social Media Sites include: "Facebook Page" and Twitter account.

It is appropriate to use a public social media site for general information about happenings, current events and liturgical information, saints of the day, surveys, etc. For example, post information you would want to appear on the front page of a local newspaper or on the broadcast news.

When setting up a public site, it is best to limit the level of participation of the members who join this community, Any social media site that is designed for public viewing should be set up so that only the administrators is allowed to post status updates, photos, videos or other content

9.0 Group Social Media Sites

Sharing of ministry best practices, upcoming events, rules and regulations as well as the opportunity to provide input can occur through group social media sites such as discussion groups, forums, list serve groups and others. Members of this community may comment as long as they follow the comment policy.

9.1Permission Levels

The administrator of a group social media site may decide the permission level they would like to give to their members. A policy regarding permission levels should be recorded and followed by the administrator, in collaboration with his/her superior(s). The application used for these purposes must offer a tracking system.

9.2 Persons Selected for Group Participation

1. Must be within the same field or position of the administrator of the group.
2. Must request to participate and be approved by administrator, or be invited to participate by the site administrator.
3. Pastor and immediate supervisor should have ability to access group, and requirement of a minimum of 2 administrators should be maintained.

9.3 Monitoring of Group Speak

1. Administrators should monitor comments posted and make sure they are respectful and appropriate to the topic.
2. Administrator should request a stop date for comments when a topic is time- sensitive.
3. Administrator should create a summary report of comments and any conclusions drawn and record these with the pastor or immediate supervisor, etc.

10.0 Personal Social Media Sites

Personal Social Media Sites are created by an individual to stay connected with family, friends, and interact with the online community—not for the purpose of ministry. Personal Social Media Sites of persons who are not clergy or religious, such as Employees, Consultants, Volunteers or other Church Personnel, should not be used for ministry or for Diocesan business purposes. Such persons should not represent their communications on their Personal Social Media Sites as official communications from the Diocese. All ministry or Diocesan business should be conducted through the official Social Media Sites of the entity to which the individual is assigned. Consequently, Personal Social Media Sites should adhere to the following guidelines:

i. The use of diocesan or church logos and trademarks is strictly prohibited.
ii. Photographs shall not offer images of ministry, church personnel or volunteers or Church structures.
iii. Ensure transparency: no anonymity or pseudonyms.
iv. Do not disclose confidential information or strictly internal Diocese matters.
v. Any Catholic, living out his/her baptismal call, would hold him/herself as a representative of the Catholic Church and a Personal Social Media Site would reflect this.

11.0 Youth and Social Media

Any media can pose dangers to individuals, particularly in a social setting. The technology which allows young people to foster friendships can also lead to cyberbullying and make them vulnerable to predators. It is everyone's responsibility to safeguard our vulnerable populations. Each Diocesan entity should educate its adult and minor members and parents and students about best practices when using social media. This education would remind parents to be aware of the on-line activities of their children. Each school and faith formation program must offer a safe environment program for parents and students.

11.1 Language Confusion

It is essential to maintain appropriate boundaries between young people and ministry leaders.

1. Appropriate boundaries are essential to all who serve in a ministerial role, and are to be observed in regards to social media as well.

2. The role of 'minister' is distinct from 'counselor', 'friend' and 'parent'. One ministering with young people should never take on the role of 'surrogate parent'. For this reason ministers are highly discouraged from 'trolling' social media with the intent of seeking personal details of a young person's life. While on-line statements are not private, it is the parents' role to monitor their child's behavior, and a minister is not to usurp this role. Intentionally monitoring where youth have shared intimate thoughts violates privacy in the same way that it would to read a journal.

3. Any information encountered within social media that creates a pastoral concern in regard to a minor should be immediately reported to appropriate authorities. Parents are to be informed immediately and legal authorities should be contacted as necessary.
4. To protect both adults and youth, ministers communicating with young people should avoid doing so with excessive frequency and at inappropriate hours. This applies regardless of the form of communication utilized.
5. Those serving in ministry are obligated to consistently represent the teachings of the Roman Catholic Church when using social media. To professionally maintain the trust of the church community, all communication is to be a tool of evangelization.
6. Healthy boundaries between youth and adults are essential. To be a 'friend' to a youth in a ministerial role is to be 'friendly' but is not to establish a peer relationship. A minister serves as a mentor and guide, walking with a young person as they journey in faith. Church Personnel are not allowed to be "friends" online with those under the age of 18. (See General Standard 3.4)
7. Church Personnel must say "no" if asked to be a friend on a personal social media site of a parent, student, parishioner or other individual who interacts with them only through this leadership role. (See General Standard 3.4)

11.2 Transparency

It is essential to the nature of ministry that parents/guardians are fully aware of all media being used to keep in contact with their young person for ministerial purposes.
The intent of any communication policy is that we give witness to the Good News in such a way that we create a safe environment for all vulnerable populations, which is open, transparent and involves the parents/guardians of the young people as partners.
It is important that ministry is not used to establish private one-on-one relationships with youth and our methods of communication must reflect this.

Unusual circumstances of a pastoral nature should be documented and shared with the pastor or one's supervisor as soon as feasible. The documentation of any such circumstance should involve a copy of any applicable communication from all types of communication medium.

12.0 What To Do Before Starting A Social Media Site

Any diocesan entity who feels the need to implement a new social media solution must first thoroughly evaluate the application to be certain it includes the functionality to be compliant with diocesan social media policy. The Office of Communications, Information Technology and Instructional Technology is available to assist with the evaluation of these opportunities. Diocesan entities are asked to inform the Diocese of Orlando Office of Communications and Information Technology when a new social media solution is discovered to allow the diocese at large to benefit from new technology that can enhance communication and evangelization.

Diocesan Network Acceptable Use Policy

1.0 Overview

The Diocese of Orlando recognizes that the Network/Internet and other emerging technologies allow authorized users access to immense information globally. The Diocese of Orlando's goal in providing this privilege to authorized users is to promote professional excellence, innovation, and communication. The use of the Network/Internet or other emerging technologies will be guided by the Diocesan Network Acceptable Use Policy (DNAUP). All Diocese of Orlando authorized users are required to sign a written DNAUP and to abide by the terms and conditions of the policy and its accompanying regulations.

2.0 Purpose

The purpose of this DNAUP is not to impose restrictions that are contrary to an established culture of openness, transparency, trust and integrity. Rather, the Diocese of Orlando is committed to protecting its authorized users from illegal or damaging actions by individuals, either knowingly or unknowingly.

These rules are in place to protect authorized users and Diocesan entities. Inappropriate use exposes Diocesan entities to risks including virus attacks, compromise of network systems and services, and legal issues. Anyone with knowledge of inappropriate material/content should report this information verbally and in writing to the IT specialist or the principal, pastor, or lay person in charge of the school, parish or ministry of the Diocese.

3.0 Policy

3.1 General Use and Ownership

1. Authorized users should be aware that the data they create on systems remains the property of the Diocesan entity. Because of the need to protect the network, management cannot guarantee the confidentiality of information stored on any network device belonging to a Diocesan entity.

2. Authorized users are responsible for exercising good judgment regarding the reasonableness of personal use. Authorized users should be guided by diocesan policies on personal use, and if there is any uncertainty, authorized users should consult their supervisor or manager.

3. The Diocese of Orlando recommends that any information that users consider sensitive or vulnerable be encrypted, especially when stored on external media.

4. Authorized personnel may monitor equipment, systems and network traffic at any time. The Diocese of Orlando maintains the right to monitor all network/computer activity derived from or utilized through its resources, whether it is on-line, down-loaded or through printed material.

5. The Diocese of Orlando, through its entities, reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6. Authorized users are advised that a determined individual may be able to gain access to services on the Network/Internet and other technologies which the Diocese of Orlando has not authorized for professional purposes. By participating in the use of the Network/Internet or other technologies, authorized users may gain access to information and communications which the authorized user may find inappropriate, offensive or controversial. Authorized users assume this risk by consenting to the use of the Network/Internet with the Diocese of Orlando.

7. Anyone who removes diocesan equipment from the business location is required to sign the Receipt of Computer Equipment form. This would include employees who require equipment while working away from the office. If equipment is removed for repair the Receipt of Computer Equipment form or appropriate receipt from vendor can be used.

3.2 Security and Proprietary Information

1. Anyone responsible for entering information into a database or have access to database information used by any Diocesan entity, whether clergy, religious, employee or volunteer, must be FBI fingerprinted and background checked and cleared.

2. The appropriate IT authority of each Diocesan entity does everything possible to ensure the Diocesan entity network is properly maintained and adequate security measures are operational. To assist the appropriate IT authority of each Diocesan entity in sustaining this goal, authorized users, through their supervisor, should notify their IT authority when software and hardware modifications are necessary on any Diocesan computer workstation. At no time should a computer be connected to a Diocesan entity network without knowledge of the IT authority of the Diocesan entity.

At no time should a computer be connected to a Diocesan entity network without the advanced knowledge and approval of that Diocesan entity's recognized IT authority. Connecting computers and peripheral devices not owned by the Diocese of Orlando (unauthorized devices) to a Diocesan entity network is prohibited unless approved in advance. This includes, but is not limited to, personal computers, printers, flash drives or other external storage devices, switches, routers and wireless equipment. Requests to connect unauthorized devices will be evaluated on a case by case basis.

The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by school confidentiality guidelines. Staff and students should take all necessary steps to prevent unauthorized access to this information.

3. Passwords will be created by each authorized users for their own use, with the exception of students, volunteers, and temporary/contractual personnel. Authorized user passwords shall not be shared. It is the responsibility of each authorized user to keep his/her password confidential. Anyone whose password becomes known to any other person should notify the appropriate authority immediately and a new password will be created. Anyone who becomes aware of anyone else's password should contact the appropriate authority immediately and a new password will be created. Temporary passwords used by students, volunteers or temporary/contractual personnel may be known by the appropriate authority. However, temporary passwords should not be shared. System passwords should be changed quarterly; user level passwords should be changed every six months.

4. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

5. Because information contained on external media is especially vulnerable, special care should be exercised to protect it in accordance to this policy.

6. Postings by authorized users from any Diocesan email address to on-line bulletin boards, forums, chat rooms, web logs ("blogs")" and any other similar non-work-related discussion groups is prohibited, unless it is specifically work related.

7. All hosts used by the authorized user that are connected to any Diocesan Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.

8. Authorized users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

9. Whenever sending "blast" e-mails or e-mails to many recipients, use the blind copy (bc) for the recipients to ensure respecting the privacy of each individual address.

3.3 Unacceptable Use

1. A database of subscribers for parish or other Diocesan use can be a useful tool for parish or Diocesan entity distribution of important messages, calendar of events, or other data. The marketplace is full of companies which offer such database opportunities. This type of database can also compromise a person's identity and/or place an individual in danger, if the database is mis-used or shared indiscreetly. No Diocesan entity should create or subscribe to a vehicle by which subscribers, other than authorized personnel such as employees, priests, deacons, religious or those designated at the discretion of the pastor or Diocesan entity head, are given e-mail addresses to communicate with other subscribers. This does not apply to instructional technology or methodology which includes approved, subscriber access for a specific instructional purpose and is monitored for this purpose. This instructional technology should not offer chat or chat rooms separate from the monitored purpose. In addition, the application should NOT without the written and express permission of each subscriber of the database:

a. Offer Chat or Chat Rooms
b. Allow Blogs (unless for educational purposes and monitored by teacher)
c. Require or Request Photos of Subscriber
d. Require or Request Video of Subscriber
e. Ask for Age or Gender of Subscriber
f. Display Subscriber E-Mail Addresses
g. Allow Subscribers Access to Other Subscriber Information

2. The following activities are, in general, prohibited. Authorized users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

a. Under no circumstances is an authorized user allowed to engage in any activity that is illegal under local, state, federal or international law while utilizing the Diocesan entity-owned resources.

b. Authorized users are prohibited from attempting to circumvent or subvert any system's security measures. Authorized users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

c. When an authorized user becomes "unauthorized" by virtue of employment, dismissal, graduation, retirement, etc., or if the authorized user is assigned a new position and/or responsibilities within the Diocesan system, his/her access authorization will automatically be reviewed with the appropriate individual to determine whether continued access is warranted. This person may not use facilities, accounts, access codes, privileges or information for which he/she has not been authorized.

d. System and Network Activities: The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Diocesan entity.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Diocesan entity or the end user does not have an active license is strictly prohibited. Public disclosure of information about programs (e.g. source code) without the owner's authorization is prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. The installation or use of Instant Messaging is prohibited.

7. Using a Diocesan computing asset to access inappropriate or offensive material or to engage in the procuring or transmitting of material that violates Diocesan anti-harassment or hostile environment policies.

8. Making fraudulent offers of products, items, or services originating from any Diocesan entity account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the authorized user is not an intended recipient or logging into a server or account that the authorized user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, creating or propagating viruses, hacking, network sniffing, spamming, pinged floods, packet spoofing, password grabbing, disk scavenging, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Diocese of Orlando is made.

12. Executing any form of network monitoring which will intercept data not intended for the authorized user's host, unless this activity is a part of the authorized user's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

e. Employee Responsibilities:

1. Privacy: No authorized user should view, copy, alter or destroy another's personal electronic files without permission.

2. Harassment, Libel and Slander: Under no circumstances, may any authorized user use Diocese of Orlando computers or networks resources to libel, slander, or harass any other person.

3. Abuse of Computer Resources: Abuse of Diocese of Orlando computer resources are prohibited. This abuse includes, but is not limited to, the following:

a. Game Playing: Installing or playing recreational games, which is not part of authorized and assigned job-related activity, are considered unacceptable practices and are prohibited during normal work hours.

b. Chain Letters: The propagation of chain letters (e-mail), "Ponzi" or other "pyramid" schemes of any type are considered an unacceptable practice and are prohibited.
c. Unauthorized Servers: The establishment of a background process that services incoming requests from anonymous diocesan employees for purposes of music/radio/video continuous Internet connectivity, chatting or browsing the Internet is prohibited.
d. Unauthorized Monitoring: An employee may not use computing resources for unauthorized monitoring of electronic communications of other employees.
e. Private Commercial Purposes: The computing resources of Diocese of Orlando shall not be used for personal or private commercial purposes or for financial gain.

3.4 Email and Communications Activities: Diocesan entities maintain electronic mail systems. These systems are provided by the Diocesan entity to assist in conducting business within the Diocese.
1. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is not allowed.
2. Unauthorized use, or forging, of email header information is not allowed.
3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is not allowed.
4. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam) is not allowed.
5. The electronic mail system hardware is the property of the Diocesan entity. Additionally, all messages composed, sent or received on the electronic mail system are and remain the property of the Diocesan entity. The Diocese, through the appropriate authority, reserves the right to review, audit, intercept, and access all messages created, received or sent over the electronic mail system for any purpose.

6. The e-mail system was created to facilitate operations of the Diocesan entity. It should be used primarily for business purposes, and only incidentally for personal use. Likewise, personal e-mail through such networks as AOL, Yahoo, Gmail, should be accessed on a limited basis.
7. The electronic mail system may not be used to solicit or proselytize for commercial ventures, political causes, outside organizations or other non-job related solicitations.
8. The electronic mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.
9. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

10. Notwithstanding the Diocese's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other authorized users and accessed only by the intended recipient. Authorized users are not authorized to retrieve or read any e-mail messages that are not sent to them.

11. Authorized users shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Authorized users should not attempt to gain access to another authorized user's messages without the latter's permission.

12. All authorized users should perform routine maintenance of their mailboxes and delete messages they are no longer using.

13. The appropriate authority should be notified if a user becomes aware of e-mails which violate this policy.

14. When communicating to a minor through any correspondence such as regular mail, e-mail, text or other technological opportunities for correspondence, such as educational programs, etc., the correspondence must be accompanied by a corresponding copy to the parent.

15. It is the responsibility of the minister or entity to collect parent e-mail addresses and monitor correspondence to be sure parents receive notification at the same time a minor notification is sent.

16. All correspondence must be professional in nature and appropriate for the ministry from which it was sent.

17. Each Diocesan Entity must have a registered domain name that provides appropriate identification of the entity. The preferable Top Level Domain (TLD) is ".org" which is appropriate for nonprofit organizations. All domain names must be registered in the name of the Diocesan entity and not be registered in the name of an individual. Domain registrations can be set to "auto-renew" with the registrar. The auto-renew feature will help prevent domains from expiring unintentionally.

18. Business email accounts must only be provided to approved employees. The creation of business email accounts for employees must be approved in writing by the Pastor or Administrator. Temporary employees and interns can be issued an email account that uses the official domain but the email address should be generic in nature and should not identify the person by name. (e.g., receptionist@orlandodiocese.org, intern@orlandodiocese.org, etc.)

19. Business email accounts must use the domain referred to in the paragraph above. Business email should not use generic domains such as yahoo.com, gmail.com, hotmail.com, etc.

4.0 System Back-up(s)

Although system back-ups should be provided by the Diocesan entity as standard operating procedure, it is the responsibility of each authorized user to backup his/her specific computer workstation data. Depending upon the amount of the individual workstation usage, workstation backups should occur daily.

5.0 Virus Protection

All networked computers must have current virus protection software installed and operational at all times.

6.0 How to Comply With The Children's Online Privacy Protection Rule

In order to provide interactive service, Diocesan entities might collect personally-identifiable information from the users the website. If such information is collected, the user will be informed about this practice. Additionally, if a website is directed to children or if a general audience website collects personal information from children, the Diocesan entity must comply with the Diocese of Orlando on-line privacy policy. The privacy policy is posted on the Diocese of Orlando website, www.orlandodiocese.org.

Digital Media and Correspondence Policy

1.0 Phone Calls to Minors

Calls should be made to a young person's home rather than to their personal cell phone in order to further transparency. If you speak with a parent/guardian, and in hearing the information you wish to share the parent/guardian asks that you contact the young person directly by the young person's cell phone, you may feel free to do so.

1.1 Calls may provide an opportunity to connect with the parents/guardians as well, and this is a helpful point of connection for family and the ministry.
1.2 Phone calls to a young person should be connected to the ministry setting, and again follow the principles of transparency.
1.3 When you are contacted by a young person be sure to observe the principles of transparency and conduct the conversation as an aspect of the ministry and be present to the conversation as a minister.
1.4 For trips off of church property it is appropriate that youth be given the cell phone numbers of the adult leaders to have in case of emergency, e.g. on an excursion to a theme park. It is also appropriate that, after parents/guardians have been informed, youth cell phone numbers are collected for use that day to ensure safety, following the guidelines of transparency.

2.0 Cards and Letters

A consistent practice of acknowledging and affirming achievements in the lives of those within ministry is certainly appropriate, e.g. sending a note to all graduating seniors or to each young person on their birthday. Communication of this type should be completely transparent and appropriate to a ministry setting. In signing your name it is appropriate to include your title and the name of the ministry you serve.

2.1 Within ministry other occasions may arise in which all youth attending an event receive a short note of affirmation in the context of our faith. This might include *palanca* notes on retreat or an affirmation activity within a program or event. Use good judgment in integrating the outlined aspects of transparency into all of your communications with youth.

3.0 E-mail to Minors

Ministry Leaders should not use their personal e-mail account for their ministry work. The parish should provide each minister with an e-mail account for ministry work and a record of this account reflected in directory information. All e-mail correspondence to a minor must be accompanied by a corresponding copy to the parent/guardian. This will require collecting e-mail information from both parents/guardians and teens at the time of registration for a program/event.

4.0 Text Messaging to Minors

Text messaging should follow the guidelines applicable to other forms of communication, including integrating the principles of transparency. Ministry Leaders and ministry team members should avoid private text communication with any minors. Communicating with youth regarding a ministry event should include copying a text message to the parent/guardian or forwarding the text message to the parent/guardian of the youth through e-mail. Communicating with a group of youth through text messaging may be done as long as parents/guardians are included in the text recipients or are sent an e-mail with the content of the text message, e.g. sending out a reflection or scripture of the day to all youth or providing information on an upcoming event.

5.0 Use of Movies Within Ministry

5.1 Showing movies/clips: Parental/guardian consent forms must be completed before showing any portion of a film rated ―R‖ on the Motion Picture Association of America (MPAA) rating scale to high school age students. This impacts film use within all high school youth ministry programs. The title of the film that will be shown, in whole or part, may be included on the overall parental/guardian consent form for a specific event. If this is a specific evening within a youth ministry planned pattern of gathering a specific parental/guardian consent form should be completed.

5.2 No portion of a film rated ―R‖ on the MPAA rating scale may be shown to students under high school age. This impacts film use within all middle school youth ministry

programs.
5.3 Parental/guardian consent forms must be completed before showing any portion of a film rated ―PG-13‖ on the Motion Picture Association of America rating scale to those under the age of 14. This impacts film use within all middle school youth ministry programs. The title of the film that will be shown, in whole or part, may be included on the overall parental/guardian consent form for a specific event. If this is a specific evening within a youth ministry planned pattern of gathering a specific parental/guardian consent form should be completed.
5.3.a *Best Practice*—Consult the Catholic News Services movie rating guide, found at www.catholicnews.com/movies.htm before deciding whether or not any clip is appropriate for use within a ministry setting. The USCCB rating system will make note of where a film reinforces or detracts from Gospel values. This system will also indicate films which the MPAA finds age appropriate, that are contrary to the faith. It will also point out films with a high level of resonance with moral and spiritual values of our faith.
5.3.b *Best Practice*—Use clips only from films with which you would be comfortable having the young person recommend to their parents/guardian for viewing the complete film.
5.4 Copyright – CVLI Church Video License provides legal coverage for churches and for other ministry organizations to show motion pictures and other audiovisual programs intended for personal, private use only ("Videos"). (Each organization needs to be specifically covered.) Coverage includes playing just a few minutes of a movie all the way up to showing the full-length feature.

10.0 Using Music Within Ministry

Providing people with tools to access media within a Gospel framework is an excellent practice. Use of music written and/or performed by Catholics or music sung by various choirs of the Diocese provide an opportunity to share the Good News and promote the many blends of Catholic hymns and songs which are available. Using music from the popular culture must include a pre-screening of lyrics. Lyrics with obscenities, or that are demeaning to people of a specific gender, race, creed or sexual orientation, are not to be played/broadcast within the ministry setting.

Video & Webcasting Policy

Well over a quarter century ago, Pope Paul VI wrote about modern communications, "The Church would feel guilty before the Lord if she did not utilize these powerful means that human skill is daily rendering more perfect. It is through them that she proclaims "from the housetops" the message of which she is the depositary. In them she finds a modern and effective version of the pulpit. Thanks to them she succeeds in speaking to the multitudes."

The Diocese of Orlando is embracing these modern communication methods to build the Kingdom of God and share the Gospel message via the tools available through internet and video technologies.

This policy will outline the guidelines to follow when recording video and/or streaming video via the internet.

Televising/Streaming the Celebration Mass

The Diocese of Orlando acknowledges the relevant needs addressed in the Guidelines for Televising Liturgy promulgated in 1997 by the United States Conference of Catholic Bishops, "Being a part of the Sunday worshiping assembly is not always possible for all members of the community. Some people have been hospitalized, home-bound, or imprisoned and do not have the opportunity to be physically present with a regular worshiping community."

Watching recorded, televised and webcast liturgies does not satisfy our obligation to gather in person regularly for these celebrations. However, technologies available in current times provide practical alternatives to remain connected in those circumstances where personal attendance is not possible. Furthermore, all diocesan entities are directed to consider the needs of the gathered faithful who are physically present for the events first and foremost. Therefore, all decisions relating to the videotaping and internet broadcast will put the interests of the physically present ahead of the virtually present.

Acknowledging our responsibility to profess the true teaching of the Church, all material presented through the methods adopted by Diocese of Orlando entities will conform to all policies, guidelines, rules and requirements of the United States Conference of Catholic Bishops, the Diocese of Orlando and the direction of our local Bishop.

These parameters are found in a variety of promulgated documents including, but not limited to:

The Church and Internet, Pontifical Council for Social Communications, *February 22, 2002*

Guidelines for Televising Liturgy, USCCB

Diocese Network Acceptable Use Policy for All Parishes, Schools and Entities of the Diocese of Orlando.

Diocese of Orlando Social Networking Policies

These guidelines are important to maintain the spirit of Church policies particularly related to the protection of vulnerable populations, the privacy of our members and the dignity of each individual who may be involved in these social communications either as a producer, subject or recipient.

Therefore the specific adopted guidelines follow.

Webcasting and Videotaping Liturgical Celebrations

Legal Standard: The Diocese of Orlando recognizes the legal standard which regulates the right to videotape and broadcast persons in public situations. Specifically the legal standard provides for the acceptance of individuals to be videotaped or broadcast in places where cameras are plainly visible.

Desiring to fully inform our members, recognizing potential limitations of some persons to be viewed on broadcast or videotape and respecting the privacy of our members, the Diocese of Orlando adopts these additional guidelines.

Webcasting and Videotaping Mass

Notice of Webcasting and Videotaping

Parishes should adopt a specific Mass or Masses which will be regularly Webcast and notice of these Masses will be provided to members at least two weeks before regularly scheduled programming begins. Additionally immediately prior to the start of any liturgy or event begins, an announcement will be made to the congregants/participants that webcasting and/or videotaping will be taking place. This notice also should be included in the written Mass program.

Permission will be deemed granted for large group views. However for individuals and small groups which would be seen in tight frame, releases will be ascertained from the individuals or legal guardian for those under the age of 18 prior to post-editing, broadcast or posting. For example, parental release forms must be executed for Altar Servers, children's choir, and children who are part of the Offertory. Files will be maintained of these releases for a period of four years, then destroyed. This is in line with the Social Communications Diocesan Network Acceptable Use Policy which states: *Parents/guardians must sign permission slips each year for the use of video where children are present.*

Identity of Participants

In particular, the Eucharistic Celebration is one in which participation of the congregants is a key element and should be noticeable in video media. However, we also wish to respect the privacy of congregants and volunteer liturgical ministers. With these thoughts in mind we set forth the following guidelines:

Identification in title graphics:

While names of Priests, Deacons, Religious and other paid members of the Parish Staff may be specifically identified in a title graphic incorporated in the broadcast or post-editing of a video production, the names of individual congregants, and volunteer liturgical ministers will not be used in any title or graphic unless necessary for an event and in that case with the consent of the individual.

Tight Frames (from a lens perspective) and Close Ups:

In general, camera angles which include congregants will be from the back or side. However, the design of facilities does not permit assurance that faces of all congregants will be unrecognizable. However, most congregant frames will be wide or mid angle. Individual close- up views will not be used, unless agreed to by individual participants prior to the beginning of videotaping or broadcasting. For those under the age of 18, parental release forms will need to be signed, per the Diocesan Network Acceptable Use Policy which states: Parents/guardians must sign permission slips each year for the use of video where children are present.

Protection of Copyright Materials:
Recognizing the limited performance rights accorded to the parish for copyright material including music, we will make good faith efforts to protect the material we use. Specifically, liturgical events will generally be live webcast only. Events post edited for upload will be limited to those portions which do not include copyright materials. i.e. Homilies or other segments which might be recorded for training or catechetical purposes. Again, an exception would be

for events where the parish has been engaged to videotape for the private use of the individuals involved. In those cases, the individuals will agree that the recorded materials will not be replicated in any form and that they will hold harmless the parish for any liability charged against the parish. Pre-recorded music will never be inserted during webcast or videotaping of the

Mass. Legally obtained and licensed images may be used tastefully. However, it is preferable to use images from the church building and grounds where these images would be useful as such images better emphasize the live presence at Mass.

Furthermore, a disclaimer should appear on the live stream or video webpage that indicates video is the property of a Diocese of Orlando entity and duplication or retransmission without permission is prohibited.

Disclosure that Obligation to attend Mass is not satisfied:
Prior to any webcast Mass, a notice will be posted in the opening inviting the viewer to attend our Masses in person and advising them that watching the live event does not satisfy their obligation as a Catholic to attend Mass in person, celebrating as the gathered body of Christ.

Direction to Liturgical Ministers
Prior to webcasting all liturgical ministers will be made aware of the videotaping and webcasting.

Use of Titles and Graphics
The action within the celebration of Mass should be the primary focus of the broadcast for

the web viewer as it is for the congregants present. Therefore titles and graphics should be used tastefully and in a limited manner. Screen graphics and titles may be used during webcast liturgical celebrations. However, their use will be limited to introductory frames, closing frames and title graphics identifying the name and position of the Homilist. Graphics identifying the Homilist shall only be used at the start of the Homily.

Videotaping Other Events

Sacramental Events

Sacramental events in a church are meant to be public. In some situations, a Sacramental event is for immediate family members only. Depending upon the entity policy, individuals involved may be allowed to videotape events for the private use of the individuals involved or for streaming on the internet or for creating keepsake DVDs that are sold to families. In this case, an image release form for all minors must be obtained.

Group Sacramental Events

Group Sacramental Events such as First Communion and Confirmation often involve the greater parish community. Depending upon the entity policy, individuals involved may be allowed to videotape events for the private use of the individuals involved or for streaming on the internet or for creating keepsake DVDs that are sold to families. In this case, an image release form for all minors must be obtained.

Other Events

From time to time a diocesan entity may capture videotape during outreach events, social events, between Liturgical events (i.e. in the courtyard), etc. It is imperative that the Parishes recognize the difference between an event where such a videotape would be limited to a large group view and an event where views would include the recognizable faces of congregants and/or participants. Permission to videotape is only provided in the case of videotaping large group views. In such cases, the aforementioned guidelines must be observed. Videotaping an event with small groups or individuals, which would be seen in tight frame (from a camera lens perspective), requires releases from the individuals or legal guardian for those under the age of 18 prior to post-editing, broadcast or posting. This is in line with the Social Communications Diocesan Network Acceptable Use Policy which states: *Parents/guardians must sign permission slips each year for the use of video where children are present.* Files will be maintained of these releases for a period of four years, and then destroyed.

Ongoing Discernment

It is recognized that as issues arise and as technologies expand additional guidelines will need to be created so the integrity and spirit of the guidelines already provided are maintained. The intent of all policies is to honor the privacy of our members, the protection of the vulnerable populations and advances the primary mission of the Church.

Conclusion

The Church has a long history of recognizing the importance of social communications in the dissemination of the truth of Jesus Christ. As "these powerful means that human skill is daily rendering more perfect" have grown and become more accessible to the multitudes, the call of the Church to use them more effectively to "proclaim the Gospel from the rooftops" has grown in fervor. However, we also recognize that with these powerful tools, constraint, prudence and caution must be taken to assure that the message of hope and life which is Jesus Christ is not zealously pursued to the point that the message is clouded or lost in the tools and methods which are available. The abuse of these tools is readily apparent and these abuses have rendered visible many of the precautions we must take to assure the integrity of our actions and purpose.

Initiated:	August, 2009
Current:	July 9, 2014

I have read and understood the Social Communications Policies and Procedures, and agree to abide by it:

Employee Signature: ____

Employee Printed Name: ____

Employee Position: ____

Parish/Entity: ____

Date: ______________________________

Appendix B:
Student Technology Responsible Use Policy

Diocese of Orlando / Office of Catholic Schools
Student Technology Responsible Use Policy
{Date}

1.0 Introduction

{School Name} recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop 21st-century technology and communication skills.

To that end, we provide access to technologies for student and staff use.

This Technology Responsible Use Policy outlines the guidelines and behaviors that students are required to follow when using school technologies or personally owned devices on and off school campus.

- The {School Name} network is intended for educational purposes.
- All activity over the network or when using school technologies may be monitored and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources or personal devices while connected to the school network or outside network can result in disciplinary action.
- {School Name} makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the school network or other technologies are required to alert Administrator, Technology staff or teacher immediately of any concerns for safety or security.

2.0 Definitions

2.1 Authorized Users:

- **Student:** any child 18 years or younger enrolled in {School Name}
- **Faculty/Staff:** any person who is employed by {School Name} , whether part-time or full-time, who provides instruction to students

2.2 School Network: communications systems connecting two or more computers and their peripheral devices to exchange information and share resources, it includes wired and wireless

2.3 Internet: includes both external and internal access of communications and data storage equipment, either owned or reserved for use by {School Name}.

2.4 Technologies Covered: {School Name} may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more. Also, {School Name} may allow students to bring their personal devices which will also be covered by this policy.
As new technologies emerge, {School Name} will attempt to provide access to them. The policies outlined in this document are intended to cover ***all* available technologies**, not just those specifically listed.

3.0 Usage Policies

All technologies provided by the school are intended for education purposes. All students are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; do not try to get around technological protection measures; use good common sense; and ask if you do not know. In the event that the inappropriate behavior happens outside of the school and it is brought to the principal's attention, {School Name} will investigate and may have disciplinary repercussions at the discretion of the school according to the Code of Conduct.

3.1 Web Access

{School Name} provides its students with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with Diocesan Social Communication Policy, CIPA (Children's Internet Protection Act) regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely. Students are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a student believes it should not be, the student should follow school protocol to alert Technology staff or submit the site for review.

3.2 Email

{School Name} may provide students with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.
If students are provided with email accounts, they should be used with care. Students should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the school policy or the teacher.
Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

3.3 Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, {School Name} may provide students with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.
Students are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging will be monitored by teachers and the sites will be protected from outside viewers. Students should be careful not to share personally-identifying information online.

The use of personal social media sites for enjoyment is prohibited on campus during instructional hours. Students must refrain from taking and posting pictures and videos of themselves, other students or teachers at school during instructional hours.

3.4 Mobile Devices Policy

{School Name} may provide students with mobile computers or other devices to promote learning outside of the classroom. Students should abide by the same responsible use policies when using school devices off the school network as on the school network.

Students are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to the student's care. Students should report any loss, damage, or malfunction to the Technology staff immediately. Students may be financially accountable for any damage resulting from negligence or misuse.

Use of school-issued mobile devices off the school network may be monitored.

3.5 Personally-Owned Devices Policy

{School Name} may allow students to bring personally owned devices to use in the classroom after it has been approved by the Technology staff. Students should keep personally-owned devices (including laptops, tablets, e-readers, smart phones, cell phones, and smart watches) turned off and put away during school hours unless as instructed by a teacher or staff for educational purposes or in the event of an emergency.

Because of security concerns, when personally-owned mobile devices are used on campus requiring the use of data, these devices must only be on the school network, data services must be disabled and permission from the Technology staff is required. For the Technology staff to grant permission, students need to submit the required paperwork with the appropriate information such as MAC address and serial number. In some cases, a separate network may be provided for personally-owned devices.

Students must to follow the same code of conduct for use of personally owned devices on {School Name} campus or at other functions, whether on or off property, related to the {School Name}.

3.6 Security

Students are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin.

If the student believes a computer or mobile device the student is using might be infected with a virus, IT must be alerted immediately. The student must not attempt to remove the virus or download any programs to help remove the virus.

3.7 Downloads

Students should not download, attempt to download, or run .exe programs or any other executable programs over the school network or onto school resources without express permission from the Technology staff.

Students may be able to download other file types, such as images of videos. For the security of our network, download such files only from reputable sites, only for education purposes, and following copyright laws.

3.8 Netiquette

Students should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Students should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Students should use trusted sources when conducting research via the Internet and follow copyright laws for their use.

Students should also remember not to post anything online that they would not want parents, teachers, or future colleges or employers to see. Once something is online, it is out there—and can sometimes be shared and spread in ways it was never intended.

3.9 Plagiarism

Students should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Students should not take credit for things they did not create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

4.0 Personal Safety

Students should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without permission from a parent or legal guardian. Students should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Students should never agree to meet someone they meet online in real life without parental or legal guardian permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you are at school; parent or legal guardian if you are using the device at home) immediately.

5.0 Cyber Bullying

Cyber bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyber stalking are all examples of cyberbullying. Do not be mean. Do not send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

6.0 Sexting

Any student taking, disseminating, transferring, possessing, or sharing obscene, sexually oriented, lewd, or otherwise illegal images or other content, commonly referred to as “sexting,” which can include, but is not limited to, pictures of themselves, other students or friends without appropriate clothing or in compromising or suggestive positions, will be disciplined according to the Student Code of Conduct, may be required to complete an educational program related to the dangers of this type of behavior, and, in certain circumstances, may be reported to law enforcement. This type of behavior needs to be immediately reported to the parent/guardian, and if it involves other students in the school it should be reported to the teacher or principal.

7.0 Examples of Responsible Use

The student will:

- ✓ Use school technologies for school-related activities.
- ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- ✓ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of others and myself.
- ✓ Help to protect the security of school resources.

This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

8.0 Examples of Irresponsible Use

I, the student will **not**:

- ✓ Use school technologies in a way that could be personally or physically harmful.
- ✓ Attempt to find inappropriate images or content.
- ✓ Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- ✓ Try to find ways to circumvent the school's safety measures and filtering tools.
- ✓ Use school technologies to send spam or chain mail.
- ✓ Plagiarize content I find online.
- ✓ Post personally identifying information, about others or myself.
- ✓ Agree to meet someone I meet online in real life.
- ✓ Send or distribute obscene, lewd or sexually explicit images.
- ✓ Use language online that would be unacceptable in the classroom.
- ✓ Use school technologies for illegal activities or to pursue information on such activities.
- ✓ Attempt to hack or access sites, servers, or content that is not intended for my use.

This is not intended to be an exhaustive list. Students should use their own good judgment when using school technologies.

9.0 Internet Safety Plan

- ✓ {School Name} implements an effective internet filtering and reporting solution {Name Solution}, that monitors internet activity, and uses current technologies to detect inappropriate usage and block and/or filter visual depictions that are obscene, pornographic or in any way harmful to minors as defined in CIPA

- ✓ The internet filtering solution is in place to control access by minors to inappropriate matter on the Internet and the World Wide Web and restrict access to materials that may be harmful to minors
- ✓ Policies and procedures are in place that covers category blocking, automated weekly reports on internet activity, and identification of emerging threats
- ✓ School network is secure with {Name Solution} to prevent from unauthorized access, including "hacking" and other unlawful activities by minors online
- ✓ Faculty provides internet safety instruction integrated in their curriculum or as part of a technology class that covers appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms and cyber bullying
- ✓ Technology Responsible Use Policy and Internet Safety Plan will be published in the parent/student handbook and {School Name} will hold an informational meeting to address the policy.

10.0 Limitation of Liability

- ✓ {School Name} will not be responsible for damage or harm to any personal devices, files, data, or hardware brought to the school by students.
- ✓ While {School Name} employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.
- ✓ {School Name} will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

11.0 Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions at the discretion of {School Name}, according to the Code of Conduct, and including but not limited to:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution

12.0 References

- ✓ Children's Internet Protection Act – http://www.fcc.gov/cgb/consumerfacts/cipa.html , http://ifea.net/cipa.html
- ✓ Children's Online Privacy Protection Act - http://www.ftc.gov/ogc/coppa1.htm
- ✓ Protecting Children in the 21st Century - http://www.ntia.doc.gov/legacy/advisory/onlinesafety/BroadbandData_PublicLaw110-385.pdf
- ✓ Consortium for School Networking – http://www.cosn.org

I have read and understood this Responsible Use Policy and agree to abide by it:

____
(Student Printed Name)

____ _________________
(Student Signature) (Date)

I have read and discussed this Responsible Use Policy with my child:

____
(Parent/Legal Guardian Printed Name)

____ _________________
(Parent/Legal Guardian Signature) (Date)

Appendix C:
DIOCESAN CYBERSECURITY PLAN FOR CATHOLIC SCHOOLS

Table of Contents

Mission and Vision

Mission

Catholic schools in the Diocese of Orlando proclaim the Gospel message within an academic environment of excellence. We challenge students to be creative and critical thinkers who integrate faith, worship, moral leadership and compassion in order to create a more just and humane world. Cybersecurity in the Diocese of Orlando will provide secure access to systems utilizing best practices and tenets of our Catholic faith fostering a culture of security awareness and compliance in our school communities.

Vision

Our schools will be positioned to benefit and protect our stakeholders as they grow in learning responsible use of data and cyber technology throughout the Diocese of Orlando. The purpose of this plan is to ensure the secure use and handling of all school data, computer systems and networking equipment. The following objectives for a vision are encouraged at each school location in the Diocese of Orlando:

- To establish and support secure network systems, processes, and procedures and to protect all personally identifiable and confidential information that is stored, on paper or digitally, in school facilities or on school-maintained servers, computers and networks.
- To prevent any school data loss or compromises that can be caused by human error, hardware malfunction, natural disaster, security breach, etc.
- To provide expectations to all persons who are granted access to the school network and other technology resources to be careful and aware of suspicious communications and unauthorized use of school devices and the network, and to report any suspicious activity to IT director.
- To require third party vendors/contractors and volunteers that house or have access to school's personally identifiable information to sign a Confidentiality Information Agreement before accessing school systems. For vendors/contractors they must have minimum insurance requirements.
- To fully conform with all federal and state privacy and data governance laws, including: Family Educational Rights and Privacy Act, 20 U.S. Code §1232g and 34 CFR Part 99 (hereinafter "FERPA"), Children's Internet Protection Act (CIPA), and the Cybersecurity Act of 2015, known as the Cybersecurity Information Sharing Act (CISA).

- To provide professional development for staff and students regarding the importance of network security and best practices a minimum of once a year.

General Introduction/Background

District Profile

The Dioceses of Orlando was established on June 18, 1968. In 1968, there were 50 parishes with 128,000 Catholics. Prior to this, the Diocese of Orlando was part of the Diocese of St. Augustine and during this time, 30 out of our 40 schools were built. Today the Diocese of Orlando has 79 parishes, 11 missions, and two basilicas that serve more than 800,000 Catholics. The Diocese currently encompasses 9, 611 square miles in nine counties: Orange, Seminole, Lake, Brevard, Osceola, Volusia, Polk, Sumter, and Marion County. The Office of Catholic Schools (OCS) oversees 40 schools – 29 elementary schools, five high schools, one special education school, and five early learning centers, serving close to 14,000 students in grades Pre-K to 12. OCS supports approximately 1,200 teachers, administrators and staff employed in the schools.

Definitions

A. Access: To directly or indirectly use, attempt to use, instruct, communicate with, cause input to, cause output from, or otherwise make use of any resources of a computer, computer system, data network (wired and wireless), or any means of communication with any of them.

B. Authorization: Having the express or implied consent or permission of the owner, or of the person authorized by the owner, to give consent or permission to access personally identifiable information.

C. Devices: Any computer, laptop, tablet, chromebook, or communication device that stores, retrieves, processes, or transmits data using the data network.

D. Data network: The interconnection of communication or telecommunication lines between: computers; or computers and remote terminals; or the interconnection by wireless technology between: computers; or computers and remote terminals.

E. Confidential: Data, text, or computer property that is protected by a security system that clearly evidences that the owner or custodian intends that it not be available to others without the owner's or custodian's permission

F. Encryption or encrypted data: The most effective way to achieve data security. In order, to read an encrypted file, you must have access to a secret key or password that enables you to decrypt the data.

G. Personally identifiable information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data and can be considered protected data, for example, full names, home addresses, personal phone numbers, email addresses, and social security numbers.

H. Confidential information: any information that could be harmful or embarrassing if made public, such as grades, test scores, health information, family information or any other information that should remain private.

I. Security system: A computer, computer system, network, or computer property that has some form of access control technology implemented, such as encryption, password protection, other forced authentication, or access control designed to keep out unauthorized persons

J. Sensitive data: Data that contains personally identifiable information.

K. System level: Access to the system that is considered full administrative access. Includes operating system access and hosted application access.

Risk Assessment

The Diocese of Orlando, Office of Catholic Schools in conjunction with the school's technology directors conducts risk assessments using the self-administered CoSN (Consortium for School Network) Risk Assessment powered by S2. Schools can also request the Cybersecurity & Infrastructure Agency (CISA) for a free cyber hygiene service or a Diocesan approved cyber company to scan and test their network. Based on the scope of these types of risk assessments the team decided to use the Center for Internet Security (CIS) Top 18 Controls to set goals and objectives. The goals and objectives will be utilized as a checklist for cyber-insurance compliance. It is recommended to hone in the five critical security controls to eliminate the vast majority of vulnerabilities.

1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for hardware and software
4. Continuous vulnerability assessment and remediation

5. Controlled use of administrative privileges

Implementation Plan

In order to prioritize implementation of the goals and objectives, the Diocese of Orlando Office of Catholic Schools has developed implementation groups (IGs). IGs are divided into three groups based on the risk profile and resources a school has available. All schools must meet cyber insurance minimum requirements in order to be covered.

IG1: is the definition of basic cyber hygiene and represents minimum objectives for information security and cyber-insurance for all schools. The safeguards included in IG1 are what every school should apply to defend against the most common attacks in order to comply with insurance requirements. Phase 1 are the objectives in the IG1 group.

IG2: are objectives that assist the school managing IT infrastructure with multiple departments and greater risk exposure. This group will be implemented as phase 2.

IG3: these objectives assist schools with IT security levels to prevent and/or lessen the impact of sophisticated attacks.

Every school will start with IG1 as they are the foundational objectives for the cybersecurity plan. We have color coded the implementation groups and identify the objectives that go with each group to make it easy to execute the plan.

IG1 – **RED**

IG2 – **YELLOW**

IG3 - **GREEN**

Goals

Goal 1: Inventory and control of hardware assets

Objective 1.1: Actively manage (inventory, track, and correct) all hardware devices	
Objective 1.2: Establish a naming convention that makes sense and helps identify the device	
Objective 1.3: Develop a good check in/check out system and have users sign an annual agreement	
Objective 1.4: Limit access to authorized devices only, unauthorized and unmanaged devices are found and prevented from gaining access	
Objective 1.5: Missing devices from inventory are quickly identified and access terminated	

Objective 1.6: Use dynamic host configuration protocol (DHCP) logging to update hardware inventory	

Goal 2: Inventory and control of software assets

Objective 2.1: Inventory of authorized and unauthorized software	
Objective 2.2: Actively manage (inventory, track, and correct) all software on the network	
Objective 2.3: Only authorized software is installed and ensure is supported and updated	
Objective 2.4: Unauthorized software is blocked from installation or execution or removed unless it is approved by the technology director	

Goal 3: Data protection

Objective 3.1: Establish and maintain a data management process	
Objective 3.2: Establish and maintain a data inventory	
Objective 3.3: Configure data access control list	
Objective 3.4: Enforce data retention	
Objective 3.5: Securely dispose of data	
Objective 3.6: Encrypt data on end-user devices including removable media	
Objective 3.7: Encrypt sensitive data in transit	
Objective 3.8: Segment data processing and storage based on sensitivity	
Objective 3.9: Deploy a data loss prevention solution	

Goal 4: Secure configuration of hardware and software

Objective 4.1: Establish, implement, and actively manage configuration of devices, servers, workstations, networking devices, and software	
Objective 4.2: Configure automatic session locking on all devices set at 5-15 minutes	
Objective 4.3: Implement and manage a firewall on servers and end user devices	
Objective 4.4: Backup all servers and test backups at regular intervals	
Objective 4.5: Standardize secure configs of OS and software and have a standard hardened image	
Objective 4.6: Establish a process for validating and refreshing images and systems on regular basis to update security config	

Objective 4.7: Backup your config for switches, firewalls, server, desktops	
Objective 4.8: Manage default accounts on hardware and software	
Objective 4.9: Remove from configurations unnecessary open ports, default accounts, default password, and older protocols	

Goal 5: Account management

Objective 5.1: Establish and maintain an inventory of accounts	
Objective 5.2: Use unique passwords and change at regular intervals	
• Not contain significant portions of the user's account name or full name	
• Be at least eight characters in length preferably twelve	
• Contain characters from the following four categories: English upper-case characters, English lowercase character, base 10 digits, non-alphabetic character	
Objective 5.3: Disable domain accounts	
Objective 5.4: Use a tier access model to assign administrative privileges to users	
• Tier 1: end user for daily use and application access	
• Tier 2: system administration accounts use to create users, administer servers and applications	
• Tier 3: infrastructure administration used for domain controllers, firewall, and switches	
Objective 5.5: Multi-factor authentication (MFA) is enabled wherever possible (administrator accounts required)	
Objective 5.6: Process and tools are used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	

Goal 6: Access control management

Objective 6.1: Establish an access granting and revoking process	
Objective 6.2: Inbound Remote Desktop Access is not accessible via the internet, only internally and via a VPN	
Objective 6.3: Establish and maintain an inventory of authentication and authorization systems	

Goal 7: Continuous vulnerability management

Objective 7.1: Acquire, assess, and act on new information to identify and manage vulnerabilities	
Objective 7.2: Timely or automatic patching operating system on server and devices on the network to minimize the window of opportunity for attackers	
Objective 7.3: Perform automated application patch management	
Objective 7.4: Perform automated vulnerability scans of internal and external devices	
Objective 7.5: Remediate detected vulnerabilities	
Objective 7.6: Remove devices from your network that cannot be patched or are not supported any longer	

Goal 8: Audit log management

Objective 8.1: Establish and maintain an audit log management process	
Objective 8.2: Collect audit logs	
Objective 8.3: Ensure adequate audit log storage	

Goal 9: Email and web browser protections

Objective 9.1: Ensure use of only fully supported browsers and email clients	
Objective 9.2: Use DNS filtering services and a content filter to monitor and protect student browsing	
Objective 9.3: Evaluate attachments and block unnecessary file types using filtering tools	
Objective 9.4: Implement DMARC	
Objective 9.5: Restrict unnecessary or unauthorized email client extensions with quarantine service	
Objective 9.6: Deploy and maintain email server anti-malware protections	

Goal 10: Virus and Malware defenses

Objective 10.1: Deploy and maintain endpoint protection (anti-virus & anti-malware) with endpoint detection and response	
Objective 10.2: Configure automatic signature updates for anti-virus and anti-malware	

Objective 10.3: Disable autorun and autoplay for removable media	
Objective 10.4: Configure automatic anti-malware scanning of removable media	

Goal 11: Data recovery

Objective 11.1: Establish and maintain a data recovery process	
Objective 11.2: Perform automated backup and test recovery data	
Objective 11.3: Protect recovery data	
Objective 11.4: Establish and maintain an off-campus instance of recovery data	

Goal 12: Network infrastructure management

Objective 12.1: Ensure network infrastructure is up to date	
Objective 12.2: Establish and maintain a secure network architecture	
Objective 12.3: A separate wireless SSID (network name) is in use for Guest access with devices segregation	
Objective 12.4: A separate wireless SSID (network name) is in use for Faculty and Student access with WPA-Personal encryption (WPA2-Enterprise with 802.1x authentication is recommended) on the private SSID	
Objective 12.5: Establish and maintain architecture diagram(s)	
Objective 12.6: Ensure remote devices utilize a VPN and are connecting to an enterprise network authentication, authorization, and auditing infrastructure (AAA)	

Goal 13: Network monitoring and defense

Objective 13.1: Centralize security event monitoring and alerting	
Objective 13.2: Deploy a host-based and network intrusion prevention and detection solution	
Objective 13.3: Manage access control for remote assets	
Objective 13.4: Collect network traffic flow logs	

Goal 14: Security awareness and skills training

Objective 14.1: Establish and maintain an information security awareness program	
Objective 14.2: Train teachers, staff, and students to recognize social engineering attacks	

Objective 14.3: Train teachers, staff, and students on authentication best practices	
Objective 14.4: Train teachers, staff, and students on data handling best practices	
Objective 14.5: Train teachers, staff, and students on causes of unintentional data exposure	
Objective 14.6: Train teachers, staff, and students on recognizing and reporting information security incidents	
Objective 14.7: Train teachers, staff, and students on how to identify and report if their devices (personal or school owned) are missing security updates	
Objective 14.8: Train teachers, staff, and students on the dangers of connecting to and transmitting personal or school data over insecure networks	
Objective 14.9: Conduct the information security awareness and skills training once a year for all groups	

Goal 15: Service provider management

Objective 15.1: Establish and maintain an inventory of service providers and ensure they sign the Confidential Information Agreement	
Objective 15.2: Establish and maintain a service provider management policy	
Objective 15.3: Ensure service providers contracts are assessed, monitor, and up to date	

Goal 16: Application software security

Objective 16.1: Establish and maintain a secure application development process	
Objective 16.2: Establish and maintain a process to accept and address software vulnerabilities	
Objective 16.3: Establish and manage an inventory of third-party software components	
Objective 16.4: Use up to date and trusted third-party software components	
Objective 16.5: Separate production and non-production systems	

Goal 17: Information Security event response management

Objective 17.1: Designate personnel to manage information security events	
Objective 17.2: Establish and maintain contact information from the Diocese of Orlando for reporting information security incidents	
Objective 17.3: Establish and maintain a school process for reporting information security	

incidents to the Diocese of Orlando	
Objective 17.4: Assign key roles and responsibilities	
Objective 17.5: Follow the Information Security Response Policy provided by the Diocese of Orlando	

Goal 18: Simulated cyber-attack testing

Objective 18.1: Establish and maintain a simulated cyber-attack testing program	
Objective 18.2: Perform periodic internal simulated cyber-attack tests	
Objective 18.3: Remediate simulated cyber-attack test findings	
Objective 18.4: Perform periodic external simulated cyber-attack tests	

Information Security Response Policy

All schools need to abide by the Diocese of Orlando Information Security Response Policy found in Addendum A.

Helpful Resources

- CIS - https://www.cisecurity.org/
- CIS Top 18 Controls - https://www.cisecurity.org/controls/cis-controls-list/
- COSN Web Site - https://www.cosn.org/edtech-topics/cybersecurity/
- NIST - https://csrc.nist.gov/projects/risk-management
- Cyber Hygiene - https://www.cisa.gov/cyber-hygiene-services
- Cyber Resource Hub - https://www.cisa.gov/cyber-resource-hub
- COSN Cybersecurity Risk Assessment Powered by S2 - https://securitystudio.com/cosn/

Addendum A: Information Security Response Policy

Last Modified **May 2022**

Diocese of Orlando
Information Security
Response Policy

Summary

This document describes the protocol that all diocesan entities must follow related to an Information Security (InfoSec) Incident.

Definitions

InfoSec Event:

Any observable occurrence in the operations of a network or information technology service, system or data indicating that a security policy may have been violated or a security safeguard may have failed.

InfoSec Incident

An InfoSec Event that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Data Breach

A data breach can be defined as an InfoSec Incident that involves sensitive, protected, or confidential information being copied, transmitted, viewed, stolen, or used by an individual unauthorized to do so. Exposed information may include credit card numbers, personal health information, customer data, company trade secrets, or matters of national security (National Institute of Standards and Technology, Feb. 2019). InfoSec Incidents may or may not be considered a data breach.

Procedure

Individuals should not attempt to determine on their own whether an InfoSec Event constitutes an InfoSec Incident as described above. Individuals should err on the side of caution as there may be legal requirements including notification time limits, depending on the nature and severity of the incident. Any individual or third party vendor at a diocesan entity that is made aware of or suspects an InfoSec Event has occurred must immediately contact the business administrator, pastor, or principal.

If the InfoSec Event cannot be resolved by IT resources (including third party vendors) at the local level, or if it is determined that an InfoSec Incident has occurred, the InfoSec Response Manager (ISRM) or alternate must be contacted via phone call or email. If business email systems are not available, it is acceptable to use an alternate email account for this purpose. Phone calls should be attempted first to all contacts until a contact is reached. If phone attempts are unsuccessful, an email should be sent to all the contacts listed.

INFOSEC RESPONSE MANAGER

Name Jack Paige	**Email jpaige@orlandodiocese.org**
Work Phone 407-246-4839	

DIOCESAN TECHNICAL CONTACTS

Name Rick Tuano	**Email rtuano@orlandodiocese.org**
Work Phone 407-246-4872	
Name O’Neal Davidson	**Email odavidson@orlandodiocese.org**
Work Phone 407 246-4874	

SCHOOL TECHNICAL CONTACT

Name Margie Garland-Aguilar	**Email maguilar@orlandodiocese.org**
Work Phone 407-246-4901	

RISK MANAGER

Name: Tracy Dann	**Email: tdann@orlandodiocese.org**
Work Phone: 407-246-4877	

Once the incident has been reported, those reporting the incident should maintain confidentiality. The formal Diocesan Information Security Incident Response Plan will guide the process through to its conclusion.

The following pages include definitions and examples of InfoSec Events and Incidents.

Examples of an InfoSec Event:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Unexplained changes to settings
- Data appears missing or changed

Examples of an InfoSec Incident:

- Unauthorized attempts to gain access to a computer, system or the data within
- Unauthorized access to sensitive information whether physical or digital
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Infections from malware such as viruses, worms, Trojan viruses, spyware, adware, ransomware or other types of malicious software (malware)
- Non-compliance with security or privacy protocols
- Data theft, corruption or unauthorized distribution
- Loss or theft of equipment used to store or work with sensitive data
- Any notification of an InfoSec Incident from a current or prior third-party vendor

Addendum B: Confidentiality Information Agreement

CONFIDENTIALITY INFORMATION AGREEMENT

This Information Confidentiality Agreement ("the Agreement") applies to all vendors and independent contractors associated with and/or involved in the activities or affairs of John G. Noonan, as Bishop of the Diocese of Orlando, his successors in office, a corporation sole, ("the Diocese") and its associated entities that may, in the course of their work, have access to any of the items described in this agreement. This includes all activity associated with the Diocese and all entities associated with the Diocese.

______________________________ ("Vendor"), agrees to and acknowledges the following requirements in return for the Diocese granting Vendor access to any of computer systems, computer networks, or data systems of the Diocese and any of its associated entities ("Diocese Networks"):

- All access to the Diocese Networks is strictly limited to the scope of the Vendor's project and nothing in this Agreement broadens the access granted by any agreement between the Vendor and the Diocese or its associated entities.
- All data, materials, knowledge and information generated through, originating from, or having to do with the Diocese Networks is the sole property of the Diocese and its associated entities.
- All data, materials, knowledge and information generated through, originating from, or having to do with the Diocese Networks is confidential and is not to be disclosed to any third party, collected, stored or maintained without the specific written consent of the Diocese. This includes, but is not limited to, all pages, forms, information, designs, documents, printed matter, policies and procedures, conversations, messages (received or transmitted), resources, contacts, e-mail lists, client information, student information, employee information, religious information, parishioner information, e-mail messages, financial information, and any information of, or relating to, the operations and activities of the Diocese and its associated entities.
- The confidential and proprietary nature of the Diocese Networks extends to all forms and formats in which the information is maintained and stored, including, but not limited to hardcopy, photocopy, microform, automated and/or electronic form.
- Any prohibited disclosure, misappropriation, prohibited copying or transmitting of any material, data or information within the Diocese Networks, whether intentional or unintentional, is a breach of this Agreement and may subject you to legal action that could include prosecution, according to the procedures set by the Diocese of Orlando and any applicable laws.
- In school settings, in addition to the requirements above, Vendor agrees l to comply with school, state and federal confidentiality laws including, but not limited to, the Family Education Rights and Privacy Act (FERPA), Protection of Pupil rights Amendment (PPRA), Children's Online Privacy Protection Act (COPPA) and the Florida Statutes and Rules on Student Data Privacy.

My signature signifies Vendor's agreement to the terms and requirements of this Information Confidentiality Agreement for Vendors.

____ ____________

Signature of Vendor/Vendor/Printed Vendor Name Date

By its:

____ ____________

Title of individual signing for Vendor Date