

# DIOCESE OF ORLANDO



## DIOCESAN TECHNOLOGY PLAN FOR SCHOOLS

Approved by: *Nicholas M. Wolsonovich*

Revision 2008

# Table of Contents

Mission and Vision .....	1
Mission.....	1
Vision.....	1
Beliefs.....	1
General Introduction/Background.....	2
District Profile .....	2
Planning Process .....	4
Needs Assessment/Goals.....	5
Funding Plan.....	11
Technology Acquisition Plan .....	11
Access .....	12
User Support Plan.....	13
Staff Training Plan .....	13
Program Evaluation Plan.....	14
Appendix A Diocesan Network Acceptable Use Policy.....	16

## **Mission and Vision**

### ***Mission***

Catholic schools in the Diocese of Orlando proclaim the Gospel message within an academic environment of excellence that challenges students to be creative and critical thinkers who integrate faith, moral leadership and compassionate service in order to create a more just and humane world. Technology in the Diocese of Orlando will support, enhance and optimize the educational endeavors of all schools, in a coordinated fashion, encompassing all grade levels, staff, disciplines, and programs. Technology will be implemented as everyday experiences and will promote higher student achievement.

### ***Vision***

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

- To provide access to state of the art technology/technological development for use with all students and staff.
- To use current and emerging technologies to enhance educational opportunities for all students, K through 12, in all subject areas.
- To use technology to increase exposure to other cultural, political and geographic areas therefore enhancing students awareness of the global community of which they are a part.
- To provide opportunities for staff development for all faculty and staff members.
- To encourage educational use of technology equipment students may have at home.
- To develop individual school technology plans emanating from the Diocesan Technology Plan.
- To develop an annual review procedure/system to review technological needs/equipment/programs at school sites throughout the Diocese and compare with others state and nationwide

### ***Beliefs***

The beliefs of the Diocesan Technology Advisory Committee are the following:

1. Technology will be used as a tool to integrate Diocesan curriculum. The curriculum must be the driving force for choosing both software and hardware.

2. The Media Resource staff and the Technology staff must work hand-in-hand to promote and enhance the technology program.
3. Technological staff development designed to increase teacher competency will be ongoing and required.
4. All teachers are responsible for teaching and using technology to enhance the total instructional program.
5. The position of a Diocesan technology coordinator is needed to assist schools with teacher inservice, implementation, and coordination of technology at the schools.
6. A technology coordinator is needed at the school level to provide support and training to faculty and staff and serve as a liaison between the school and the Office of Catholic Schools.
7. A technology advisory committee is needed at the school level to guide the technology coordinators and the principals in the decision making process for technology acquisition.

### **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 37 schools were built. Today the Diocese of Orlando has 80 parishes and 10 missions that serve more than 800,000 Catholics. The Diocese currently encompasses 11,255.66 square miles in nine counties: Orange, Seminole, Lake, Brevard, Osceola, Volusia, Polk, Sumter, and Marion County. The Office of Catholic Schools oversees 37 schools – 31 elementary schools, five high schools and one special education school, serving close to 15,000 students in grades PreK to 12. OCS supports approximately 1,200 teachers, 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, and the Research Park, 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	18	2	20
Inner City	1	0	1
Suburban	12	2	14
Rural	1	1	2
Total	32	5	37

Elementary Schools PK-8 Enrollment by Ethnicity 2008-2009

	CATHOLIC	NON- CATHOLIC	UNKNOWN	Total
NATIVE AMERICAN	14	4	2	18
ASIAN	502	76	0	562
BLACK	273	166	1	365
HISPANIC	1970	63	0	1936
NATIVE HAWAII /PAC ISL	82	0	0	127
WHITE	7445	670	15	8375
MULTI-RACIAL	335	44	1	389
UNKNOWN	39	4	2	29
TOTAL	10,660	1,027	162	11,849

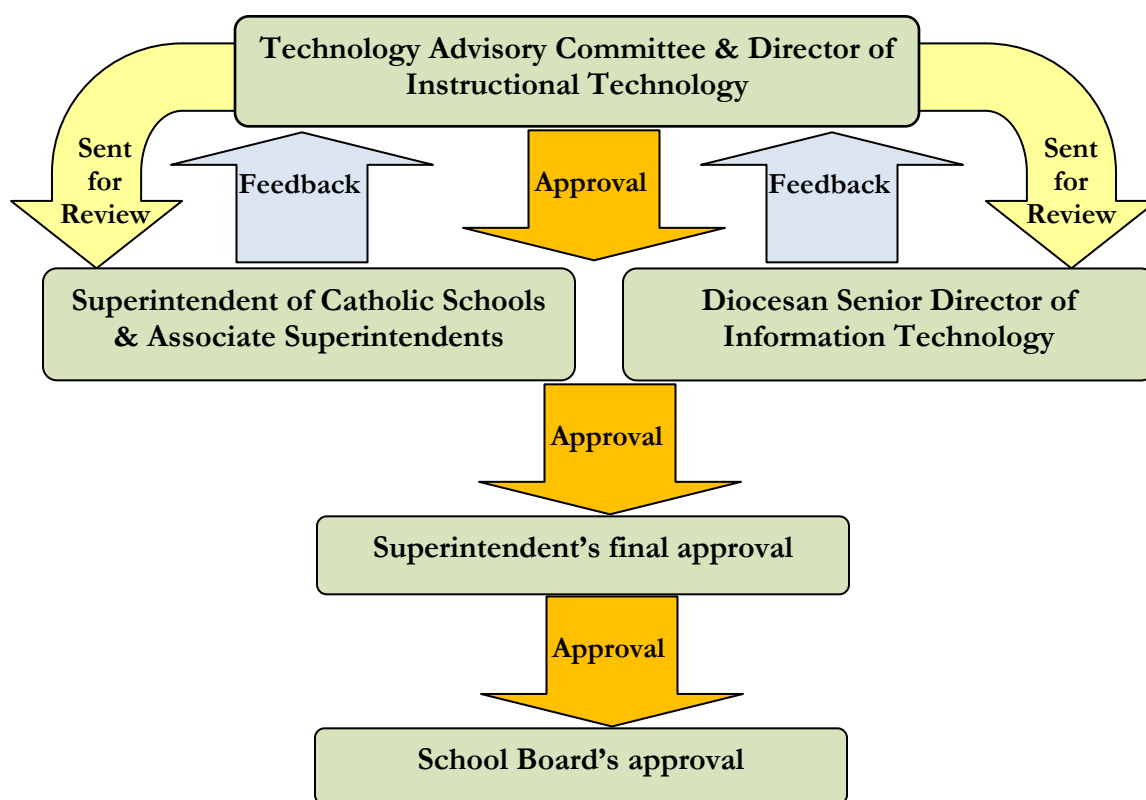
High Schools Enrollment by Ethnicity 2008-2009

	CATHOLIC	NON- CATHOLIC	UNKNOWN	Total
NATIVE AMERICAN	3	0	0	3
ASIAN	72	13	1	86
BLACK	59	40	1	100
HISPANIC	385	5	0	390
NATIVE HAWAII/ PACIFIC ISL	9	1	0	10
WHITE	1765	203	3	1971
MULTI-RACIAL	109	12	0	121
UNKNOWN	34	8	4	46
TOTAL	2,436	282	9	2,727

19 out of our 37 schools in the Diocese have received the U.S. Department of Education No Child Left Behind Blue Ribbon School Award.

**Planning Process**

During the spring 2008, a “Technology Advisory Committee” was formed to improve the 2002 Diocesan Technology Plan, provide direction on specific technologies, and how technology is used in the district. The revised plan will provide guidance for schools in the Diocese of Orlando to implement and maximize technology. The committee members will meet four times a year, and they are School Technology Coordinators representing each of the regions of the Diocese. This committee will work with the Diocese’s Director of Instructional Technology and members of the Diocesan School Board Communications Sub-Committee. The approval process for the technology plan includes review and acceptance by the following groups:



Technology Advisory Committee	
Margie Aguilar	Office of Catholic Schools
Anita Brady	Ascension Catholic School, Brevard County
Scott Ebert	Trinity Catholic High School, Lake & Marion County
Jim Durbin	St. Charles Borromeo Catholic School, Orange County
Ken Hjortsberg	St. John Vianney Catholic School, Orange County
Melissa Hager	Resurrection Catholic School, Polk County
Lisa Jones	Annunciation Catholic Academy, Seminole County
Eileen Baines	St. Peter Catholic School, Volusia County

<b>Diocese of Orlando</b>	
Dr. Nicholas Wolsonovich	Secretary of Faith Formation / Superintendent of Catholic Schools
Mr. James Cooney	Associate Superintendent for Curriculum
Sr. Rosemary Hickmann	Associate Superintendent for Staff Development
Margie Aguilar	Director of Instructional Technology
Jack Paige	Senior Director of Information Technology

### **Needs Assessment/Goals**

The Diocese of Orlando, Office of Catholic Schools utilized the goals and requirements described by 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. Also, short-term and long-term goals were created to meet our schools' needs. Each school will develop a technology plan based on the goals and objectives of the Diocesan Technology Plan. The Office of Catholic Schools encourages a single source vendor program and joining the Mid-South Independent School Business Officers (MISBO) to participate in cooperative procurement. The Technology Advisory Committee identified five major goals.

### **Goal 1: Improve Student Learning with Technology Opportunities and Experiences**

Objective 1: Implement technology enhanced classrooms through product evaluation and standardization. The classrooms will have the basic components of a 21<sup>st</sup> Century classroom with all multimedia equipment. Suggestions of equipment for the classrooms are the following:

- Mounted LCD Video Projector minimum 2500 lumens
- 5 – 7 feet mounted Projection Screen
- Digital Document Camera
- DVD/VCR Player with digital tuner
- Audio Enhancement Equipment
- Networked Desktop / Laptop or Tablet for Teacher workstation
- Optional Electronic Whiteboard or Tablet with software
- Optional Response Systems preferably RF

Objective 2: Offer students at least a computer per five students and maintain a refresh program, replacing computers every 3 to 5 years in the classrooms, computer labs, and media centers.

Minimum specifications for student stations are:

- Intel Core 2 Duo Processor (2.0 GHz, 4 MB L2 Cache, 800 MHz FSB)
- 2.0 GB DDR2 SDRAM
- 80 GB SATA 7200 RPM Hard Drive
- 16 X DVD+/- RW SATA
- Integrated Graphics Card
- Wireless Card
- LAN Card
- 3 to 4 Year Warranty

Objective 3: Schools need to develop and maintain a set of technology benchmarks for students based on ISTE standards and provide an assessment to students as they reach eighth grade for technology proficiency.

Objective 4: Encourage the use of technology materials that accompany textbooks, reference data bases and web-based applications and train teachers, students, and parents.

Objective 5: Promote the use of new global communication technologies to allow for online collaboration and global awareness, as long as it is monitored by the teacher. Examples are:

- Web blog
- Audio / Video Broadcast like RSS and podcasting
- Social bookmarking
- Online discussions
- Electronic portfolios

Objective 6: Implement at least one wireless mobile lab of 30 laptops for each school. This will allow teachers in all subject areas to engage students and integrate technology in their curriculum.

Minimum requirements for the laptops are:

- Core 2 Duo Processor (2.4GHz,4MB L2 Cache, 800Mhz FSB)
- 15.4 Screen
- 2.0 GB DDR2 SDRAM
- 80 GB SATA 7200 RPM Hard Drive

- 16 X DVD+/- RW SATA
- Integrated Graphics Card
- Wireless Card
- LAN Card
- Battery
- AC Adapter
- 3 to 4 Year Warranty

Objective 7: Develop a Distance Learning Program using video conferencing equipment to provide students with educational opportunities that they might not otherwise have access to due to geographical location, school size or resources. This should be implemented in phases:

- Phase 1 – high schools connected to the Chancery office
- Phase 2 – selected elementary schools with the appropriate bandwidth in each of the regions
- Phase 3 – continue upgrading infrastructures to reach all elementary schools

Objective 8: All schools in the Diocese of Orlando need to develop and implement an age appropriate internet safety curriculum. The Office of Catholic Schools recommends using NetSmartz Kids or Web Wise Kids programs.

**Goal 2: Create a Solid Network Infrastructure with Integrated Hardware and Software Systems**

Objective 1: Improve the integrity, reliability, and speed of the schools' LAN.

- Fiber connectivity should exist between buildings in the school
- Upgrade routers to support new network backbone
- Install at a minimum a gigabyte network within servers and 100 Mps to the desktop
- Install network security and intrusion detection to house wired and wireless clients
- Upgrade the infrastructure to support wireless, voice, data, and video conferencing technologies
- Install wireless network in all the schools
- Upgrade power protection in network closet
- Maintain a refresh program for network and server equipment
- Develop and update a Disaster Recovery Plan

Objective 2: The school should maintain acceptable servers and locate them in a well ventilated secured room.

- Purchase server with the requirements to run the necessary applications in the school and obtain a five year warranty
- Install and maintain antivirus on all servers
- Establish back-up procedures to ensure that server data integrity is maintained
- Provide redundancy or fault tolerance data storage on critical servers
- Put into practice Active Directory and Group Policy to manage different users on the school's network
- Upgrade power protection in server rooms as necessary
- Monitor and maintain OS with patches and updates
- Replace all essential servers at least every five years

Objective 3: Improve the integrity, reliability, and speed of the internet environment to maintain a 100% uptime.

- Monitor bandwidth and increase it as necessary to provide a stable connection
- Add network ports or wireless access points as necessary to provide a reliable connection for the devices
- Provide internet content filtering

Objective 4: Standardized all the printers throughout the school. Selecting the same brand and model of printer and making them available on the network will reduce the cost of supplies and maintenance. Also, it will reduce printing to what is necessary, thus protecting the environment. Locate the black & white printer in strategic places, maybe teachers' workroom and a color printer in the computer lab or administration offices.

Objective 5: Implement an inventory tracking software at each school site to monitor hardware and software throughout the site and manage the assets' life expectancy.

### **Goal 3: Increase Productivity for Teachers and Administrators**

Objective 1: Provide all teachers with a laptop and maintain a refresh program of three to four years.

Minimum specifications for teacher's laptops are:

- Dual Core Processor (2.4GHz, 4 MB L2 Cache, 800 MHz FSB)
- 2.0 GB DDR2 SDRAM
- 120 GB SATA 7200 RPM Hard Drive

- 16 X DVD+/- RW SATA
- Integrated Graphics Card
- Wireless Card
- LAN Card
- 3 to 4 Year Warranty

Objective 2: Provide an administrator-to-computer/laptop ratio of 1:1 at all schools and maintain a refresh program of three to four years. Minimum specifications for an administrator's workstation or laptop are:

- Dual Core Processor (2.4GHz, 4 MB L2 Cache, 800 MHz FSB)
- 2.0 GB DDR2 SDRAM
- 120 GB SATA 7200 RPM Hard Drive
- 16 X DVD+/- RW SATA
- Integrated Graphics Card
- Wireless Card
- LAN Card
- 3 to 4 Year Warranty

Objective 3: Establish a school administration software that automates data collection, storage, and reporting of the following areas: student records, admissions, accounting, attendance, report cards, development, and cafeteria at each school. This system will increase teachers' and administrators' efficiency and productivity. Also, data reports will be easier to obtain since it is an electronic database.

Objective 4: Implement a teacher online grade book in every school so they have anywhere access to student information anytime, anywhere.

Objective 5: Continue to move to web-based applications so information is accessible to administrators and teachers, increasing efficiency and improving student achievement. Examples:

- Curriculum Mapper
- Classroom Walkthrough
- Online Classroom Websites
- Online Grades

Objective 6: Develop a web portal for teachers and administrators through the OCS website to improve communication and offer additional resources.

#### **Goal 4: Enhance Parent and Community Communications**

The Diocese of Orlando recognizes that communication between schools and families is an important factor in determining student success. Excellent communication systems provide support for busy students and families and allow for greater student achievement and a happier learning environment. While recognizing that the individual needs and resources of Diocesan schools vary widely, the following objectives are recommended.

Objective 1: Implement parent-school online communication software (web-portal) for attendance, grades, homework, school information, classroom information, and teacher's websites at all schools.

Objective 2: Improve the Diocesan website with parent information and community links.

Objective 3: Improve school's website to look professional and provide information with timely updates.

Objective 4: Research instant parent notification applications via phone, text message, and email.

Objective 5: Preview communication products through the Tech Coordinators' meetings as a way to find products that are scalable and therefore usable for a wider range of schools.

Objective 6: Improve the Office of Catholic Schools website and research the feasibility of having a Diocesan portal for parents.

#### **Goal 5: Teachers and Administrators will become Effective Users of Technology to Enhance Learning**

Objective 1: Provide an annual Summer Technology Institute for teachers consisting of five days of technology instruction and curriculum integration in a hands on environment. The Diocesan Director of Instructional Technology will be in charge of organizing the training.

Objective 2: Designate a technology coordinator at each school to serve as the technology point of contact to the Office of Catholic Schools.

Objective 3: Implement an assessment tool to identify educator's technology skills. Use the results of the assessment tool to develop an individual skills improvement plan and identify training needed at each school site.

Objective 4: Provide training on integrating and emerging instructional technologies. The technology coordinator can organize local training or invite the Diocesan Director of Instructional Technology to offer instruction. During the teachers' pre-planning week, each school should provide training to review hardware and software use.

Objective 5: Develop a technology user's manual at each school with steps on how to use software, equipment, and how to do maintenance and simple troubleshooting.

Objective 6: Encourage faculty and staff to attend instructional classes or workshops by providing information concerning courses, workshops, and conferences.

Objective 7: Offer online training courses, share resources, and distance learning (video conferencing) for professional development and staff training for all employees at the Diocesan level.

### **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.

### **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 desktops and laptops for all the schools. The schools need to take advantage of buying in volume by combining purchases or leasings from one single vendor. The initiative of formalizing a uniform standard for hardware purchases ensures technology will enhance student achievement and comply with 21<sup>st</sup> Century and Florida Sunshine State Standards in the most cost effective manner.

The Diocesan Technology Advisory Committee will create a guide of recommended hardware and software products. Also, a list of approved vendors with a history of reliable products and acceptable support and training will be developed to help schools when making purchases. These guides will be posted on the Diocesan website for easy access by the school's technology coordinators. The identification of appropriate technologies will be based on recommendations from the technology coordinators at the schools.

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, support, and maintenance requirements.

### **Access**

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

Developing a refresh program to address computer and server 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 from the *Alive In Christ Campaign*. In addition, the refresh program will make available computer that are obsolete to the schools but could be given to students without access to computer 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 will be available on every school's website. Examples of some of those programs are Britannica Online, Education City, Compass Learning, Success Maker, and Kids Infobits. Also, schools need to provide access to information for decision making by teachers and administrators.

The Diocese of Orlando has developed a network acceptable use policy for access to all the systems including internet. This AUP 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 DNAUP is provided to all students, parents, teachers, and staff and signatures are collected and placed on file. Also, the document is available at <http://www.doschool.org/DNAUP%202007.htm> . The schools have to monitor and filter internet access utilizing software or hardware that blocks content that is obscene, harmful or pornographic

to minors. The Office of Catholic Schools recommends the use of Surf Control or CIPA Filter to monitor and block content not appropriate for children.

### **User Support Plan**

The Technology Advisory Committee's main goal for the user support plan was 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 teachers 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 a Online Teacher Resource Center with tutorials, assistance, and education resources for teachers and administrators.
4. Standardized the school's hardware including servers, computers, video equipment, and printers and obtain service and support.
5. Standardized the school's software, offer training, and provide with user's guide.
6. Utilize a network management software that will do network troubleshooting and repair, inventory software and hardware, allow software updates to be installed centrally, and remote access to desktop computers.
7. Develop a group of students that can help provide technology support through the school.
8. Utilize some of the Web 2.0 tools to develop collaboration between teachers and forums to share and discuss ideas.

### **Staff Training Plan**

To support the technology initiatives that are implemented within the Diocese, it is essential a comprehensive staff development plan be established. 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.

District Workshops - In 2007, the first Diocesan Summer Technology Institute was offered at the University of Central Florida. It was a five day training on different technologies and how to integrate it in the curriculum. The group was twenty-two teachers from different schools, and it was very successful. The idea is to train them and have them go back to the school and train the teachers at their site. It was offered again in 2008 with thirty participants. The Office of Catholic Schools will continue to offer the Institute to try to reach as many teachers as possible. There is a follow up session during the school year to come together and discuss some of their implementations.

Guided Modules – Training modules are developed on specific content areas that are computer based. These guided modules also support the effort to keep teachers to remain in the classroom in lieu of workshops during the school day.

School or Region Based Training – This 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.

Online Training - From the Summer Institutes, a wiki has been developed to share knowledge and resources between them. A series of self paced training modules are available through Atomic Learning, Lynda.com, and many other applications.

Another area is training for technology coordinators. Attendance at conferences like FETC and NECC is encouraged. Also, the Office of Catholic Schools provides training opportunities at the Chancery for all Technology Coordinators and their attendance is expected.

### **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 Staff Development Committee prepares an annual online survey for teachers. This survey is tabulated and the Committee can prepare a plan for staff 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 recommends implementing a Diocesan Technology Skills Assessment for students in middle school and high school. This tool is given as a pre and post test and will determine if our students are learning the standards established by the International Society for Technology in Education. This instrument also will identify areas in which teachers need training.

Appendix A  
Diocesan Network Acceptable Use Policy

**Diocese of Orlando**  
**Network Acceptable Use Policy updated 09/26/07**  
**For All Parishes, Schools and Entities of the Diocese of Orlando**

**1.0**    **Glossary of Terms**

**1.1**    **Authorized users:**

1. **"Employee"**: Any lay person who is employed by or engaged in ministry in 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).
2. **"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.
3. **"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.
4. **"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.

**1.2**    **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.

1. 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.

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

**1.4**    **Spam:** Unauthorized and/or unsolicited electronic mass mailings.

**1.5**    **IT:** Information Technology\_

**1.6**    **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.”

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

## **2.0 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.

## **3.0 Scope**

This policy applies 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.

## **4.0 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.

## **5.0 Policy**

### **5.1 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.

## **5.2 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.
3. 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.
4. 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.
5. 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.
6. Because information contained on external media is especially vulnerable, special care should be exercised to protect it in accordance to this policy.
7. 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.

8. 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.
9. 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.
10. 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.

### **5.3 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:
  - a. Offer Chat or Chat Rooms
  - b. Allow Blogs
  - c. Require or Request Photos of Subscriber
  - d. Ask for Age or Gender of Subscriber
  - e. Display Subscriber E-Mail Addresses
  - f. 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:**

- i.** Privacy: No authorized user should view, copy, alter or destroy another's personal electronic files without permission.
- ii.** 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.
- iii.** Abuse of Computer Resources: Abuse of Diocese of Orlando computer resources is prohibited. This abuse includes, but is not limited to, the following:
  - 1.** 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.
  - 2.** 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.
  - 3.** 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.

4. **Unauthorized Monitoring:** An employee may not use computing resources for unauthorized monitoring of electronic communications of other employees.
5. **Private Commercial Purposes:** The computing resources of Diocese of Orlando shall not be used for personal or private commercial purposes or for financial gain.

5.4 **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.

## **6.0 Enforcement**

Effective security is a team effort involving the participation and support of every authorized user who deals with information and/or information systems. 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 the Network/Internet and other available technology that is not authorized by or conducted strictly in compliance with this policy and its regulations. Authorized users who disregard the DNAUP may have their Network/Internet privileges suspended or revoked and may be subject to a change in their relationship with the Diocese, up to and including termination. The Diocese of Orlando reserves the right to suspend or revoke such privileges in the event that any supervisor believes the authorized user's conduct to be inappropriate or noncompliant with the DNAUP. Authorized users granted access to the Network/Internet and other technologies through Diocese of Orlando assume personal responsibility and liability, for their actions. In addition, any employee, volunteer, or contractor found to have violated this policy may be subject to disciplinary action, up to and including termination. Authorized users who have read and signed the DNAUP form and who agree to act in a considerate and responsible manner will be authorized Network/Internet access.

## **7.0 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.

## **8.0 Virus Protection**

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

## **9.0 Website Requirements**

Any website of a Diocesan entity links sites that are not in conflict with the teaching and the magisterium of the Roman Catholic Church. The 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 such as parishes, schools and ministries operated by the Diocese or approved resources associates with those ministries; and
3. 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.

4. Use of photos on websites should be group photos. Where children are involved, 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.
5. All Diocesan parishes, schools, and entities should have a link for the Diocese of Orlando website, [www.orlandodiocese.org](http://www.orlandodiocese.org), on its own website.

**10.0 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](http://www.orlandodiocese.org).

As a condition to use the Diocesan Network/Internet, I agree to abide by the terms and conditions of DNAUP, and I understand that my access may be suspended or terminated if I violate the policy.

Signed: \_\_\_\_\_  
*Name*

Printed Name: \_\_\_\_\_

Date: \_\_\_\_\_

Position: \_\_\_\_\_

Parish/Entity: \_\_\_\_\_