APPENDIX I

SERVING CHRIST, SERVING OTHERS CODE OF MINISTERIAL CONDUCT
AND
PROMISE TO PROTECT, PLEDGE TO HEAL POLICY FOR THE PROTECTION OF CHILDREN AND YOUNG PEOPLE

APPENDIX II

FAMILY AND MEDICAL LEAVE OF ABSENCE (FMLA) POLICY

General Provisions

Employees who have worked for at least one year and worked at least 1,250 hours during the previous twelve (12) months are eligible for an unpaid leave of absence in accordance with this Family and Medical Leave of Absence ("FMLA") Policy. Eligible employees may take a leave in the event of:

(a) The birth of a child, in order to care for the child (leave must be taken within twelve (12) months of the birth of an employee's child);

(b) An adoption or foster care placement of a child, in order to care for the child (leave must be taken within twelve (12) months of the adoption or placement in the employee's home);

(c) A serious health condition of the employee's spouse, child or parent when the ill person is incapable of self-care and the employee is needed for such care;

(d) A serious health condition of the employee which results in the employee's inability to perform his or her job;

(e) Any "qualifying exigency" that stems from the fact an employee's spouse, child or parent is on or has been called to "covered active duty" in the Armed Forces in support of a contingency operation;[1] or

(f) The serious injury or illness[2] of a "covered service member" who is undergoing medical treatment, recuperation, or therapy, or is on outpatient status or on the temporary disability retired list and who is the employee's spouse, son, daughter, parent, or next of kin ("nearest blood relative"), in order to care for the service member.[3]

[1] "Covered Active duty" means duty under a call or order to active duty under a provision of law referred to in section 101(a)(13)(B) of title 10, United States Code, including duty where regular service members are deployed by the Armed Forces to a foreign country. "Contingency operation" has the same meaning as that set forth in section 101(a)(13)(B) of title 10, United States Code.

[2] "Serious injury or illness" is defined as a condition that may render the service member "medically unfit to perform the duties of the member's office, grade, rank, or rating."

[3] A "covered service member" is defined as "a member of the Armed Forces, including a member of the National Guard or Reserves, who is undergoing medical treatment, recuperation, or therapy, is otherwise in outpatient status, or is otherwise on the temporary disability retired list, for a serious injury or illness." The definition also includes veterans who are undergoing medical treatment, recuperation, or therapy for a serious injury or illness and who were members of the Armed Forces (including National Guard and Reserves) during the five (5) year period preceding the date of treatment, therapy, or recuperation.

An eligible employee is entitled to a total of twelve (12) workweeks of leave for types (a) through (e) leave and twenty-six (26) workweeks of leave for type (f) leave during any twelve (12) month period. The School utilizes a "rolling" twelve (12) month period, measured backward from the date an employee uses FMLA, to calculate the amount of leave available to an employee. In other words, the number of weeks an employee has available upon the beginning of an FMLA will be twelve (12) weeks less the number of FMLA weeks taken during the previous twelve (12) months (the "available leave weeks").

For example, if an employee has taken eight (8) weeks of types (a) through (e) FMLA during the past twelve (12) months, an additional four weeks of types (a) through (e) leave could be taken when a second leave is requested. If an employee used four (4) weeks beginning February 1, 2008, four (4) weeks beginning June 1, 2008, and four (4) weeks beginning December 1, 2008, the employee would not be entitled to any additional leave until February 1, 2009. The employee would be entitled to four (4) weeks of leave beginning February 1, 2009, another four (4) weeks on June 1, 2009, and so on.

FMLA for the birth or placement for adoption/foster care of a child, as described in (a) and (b) above, must be taken all at once unless otherwise agreed to by the School. If medically necessary, FMLA due to illness, as described in (c), (d), and (e) above, may be taken on an intermittent or reduced leave schedule. If FMLA is requested on an intermittent or reduced schedule basis, the School may require the employee to transfer temporarily to an alternative position better suited for periods of absence or a part-time schedule, provided that the position has equivalent pay and benefits.

An employee's earned, unused vacation will be included as part of the twelve (12) week leave requirement for FMLA type (a), (b), (c), (e), and (f) leaves listed above. For example, an employee with two (2) weeks of earned, unused vacation is required to use that time before taking not more than ten (10) weeks of unpaid leave. For an FMLA type (d) leave, employees may use accrued sick or vacation days for the waiting period before short-term disability income benefits, if any, begin.

If the employee on FMLA is an *exempt* employee and is among the highest paid ten percent (10%) of diocesan employees within a 75-mile radius, and keeping the position open for the employee would result in substantial economic harm to the diocese, reinstatement can be denied at the end of the leave period. The School will identify such "key employees" when FMLA is initiated.

When employees request any leave of absence that qualifies as leave under FMLA, the School may designate such leave as FMLA upon written notification to the employee. The period of disability associated with pregnancy, childbirth or a work-related accident will be counted as FMLA type (d) leave.

Status of Employee Benefits

While on FMLA, employees may continue to participate in the School's group health insurance plan in the same manner as employees not on FMLA. However, an employee must pay to the School the employee's share, if any, of medical and dental insurance premiums once per month in advance on the first day of each month. At the end of an authorized FMLA, an employee will be reinstated to his/her original position or a comparable position,

In the event that the employee elects not to return to work upon completion of FMLA, the School may recover from the employee the cost of any payments to maintain the employee's medical or dental coverage, unless the employee's failure to return to work was for reasons beyond the employee's control. Benefit entitlements based on length of service will be calculated as of the last paid work day prior to the start of a leave of absence. For example, an employee on leave will not earn vacation time.

Basic Regulations and Conditions of Leave

The School may require medical certification to support a claim for FMLA for an employee's own serious health condition or to care for a seriously ill child, spouse, parent, or for service member family leave. For the employee's own medical leave, the certification must include a statement that the employee is unable to perform the functions of his/her position. For FMLA to care for a seriously ill child, spouse, parent, or family service member, the certification must include an estimate of the amount of time the employee is needed to provide care. At its discretion and expense, the School may require a second medical opinion and periodic re-certifications. If the first and second opinions differ, the School, at its own expense, may require the binding opinion of a third health care provider, approved jointly by the School and the employee. The School may require certification related to active duty or call to active duty for type (e) leave above.

Notification and Reporting Requirements

When the need for FMLA is foreseeable, such as the birth or placement for adoption/foster care of a child, planned medical treatment, "qualifying exigency," or in order to care for an injured service member, the employee must provide reasonable prior notice and make efforts to schedule the leave so as not to disrupt School operations. In cases of illness, the employee will be required to report periodically on his/her FMLA status and intent to return to work. At the conclusion of any FMLA due to the employee's own illness, the employee must present a written authorization form from his/her doctor stating that the employee is capable of returning to work.

Procedures

1. An employee will submit a Request for FMLA Leave form to the Principal (or in the case of the Principal, the Superintendent). If possible, the form should be submitted 30 days in advance of the effective date of the FMLA.

2. All requests for FMLA type (c) and (d) leaves of absence due to illness should include the following information to be supplied by the treating medical provider:

   a) The date on which the serious health condition commenced;
   b) The probable duration of the condition; and
   c) The appropriate medical facts within the knowledge of the health care provider regarding the condition.

3. In addition, for purposes of FMLA type (c) and (e) leave to care for a child, spouse or parent or covered service member, the request should give an estimate of the amount of time that the employee is needed to provide such care.

4. For purposes of FMLA type (d) leave for an employee's illness, the medical certification must state that the employee is unable to perform the functions of his/her position.

5. For purposes of FMLA type (e) and (f) leave, the request must include verification from a commanding officer.

6. In the case of certification for intermittent FMLA or FMLA on a reduced schedule for planned medical treatment, the dates on which such treatment is expected to be given and the duration of such treatment must be stated.

Coordination with Maternity Leave

The School provides employees with a leave of absence for the period of temporary physical disability resulting from childbirth and related medical conditions. A maternity leave begins when the employee is medically determined to be disabled and ends when medically determined to be able to return to work.

Maternity disability will be treated in the same manner as an FMLA type (d) leave of absence. The employee may receive short-term disability income benefits in accordance with the School's benefit package.

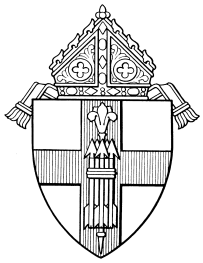
An employee who uses fewer than the available leave weeks for an FMLA type (d) leave for maternity may take additional FMLA type (a) leave after the end of the disability period up to the number of available leave weeks. The employee must utilize accrued, unused personal days or vacation time before taking any unpaid leave during the FMLA type (a) leave of absence.

Maternity leaves are not limited by any measure other than the period of medical disability. If a maternity disability is for the number of available leave weeks or less, the employee will be reinstated in accordance with this policy. If a maternity disability extends beyond the available leave weeks, the employee will be reinstated unless business necessity makes reinstatement impossible or unreasonable.

Coordination with Other Policies
Reference to Federal Law and Regulations

In the event of any conflicts between this policy and other School policies, the provisions of this policy shall govern. To the extent they are applicable, the Family and Medical Leave Act of 1993 and the federal regulations issued by the U. S. Department of Labor will be applied in instances of requested or designated FMLA.

A Request for FMLA form follows this policy statement for employees' use.



REQUEST FOR FAMILY/MEDICAL LEAVE

DATE: _____

FROM: _____

DEPARTMENT: _____

This is to request a Family and Medical Leave of Absence for the following reason (*check one)*:

- ❑ The birth of a child in order to take care of the child (leave must be taken within 12 months of the birth and child must live with employee).

- ❑ The adoption or foster care placement of a child in order to care for the child (leave must take place within 12 months of the placement in the employee's home).

- ❑ A serious health condition affecting my [ ] spouse, [ ] child, [ ] parent, because the ill person is not capable of self-care and I am needed for such care (see attached Certification of Health Care Provider.

- ❑ My serious health condition which results in my inability to perform my job (see attached Certification of Health Care Provider.

- ❑ Any "qualifying exigency" that stems from that fact a spouse, child, or parent is on or has been called to active duty in the Armed Forces in support of a contingency operation.

- ❑ The serious injury or illness of a "covered service member" who is undergoing medical treatment, recuperation, or therapy, or is on outpatient status or on the temporary disability retired list and who is my [ ] spouse, [ ] child, [ ] parent, or [ ] next of kin, and I am needed to care for the service member.

I wish to commence this leave of absence on _____

I anticipate that this leave will end on _____

_____
Employee signature

Approved by: _____

Date approved: _____

CERTIFICATION OF HEALTH CARE PROVIDER*

1. Employee's Name

2. Patient's Name (if different from employee):

3. The attached sheet describes what is meant by a "serious health condition." Does the patient's condition[1] qualify under any of the categories described? If so, please check the applicable category:

   (1)____(2)____(3)____(4)____(5)____(6)____ or None ____

4. Describe the medical facts which support your certification, including a brief statement as to how the medical facts meet the criteria of one of these categories:

5. (a) State the approximate date the condition commenced, and the probable duration of the condition (and also the probable duration of the patient's present incapacity[2] if different:

   (b) Will it be necessary for the employee to take work only intermittently or to work less than a full schedule as a result of the condition (including for treatment described in Item 6 below)? If yes, give the probable duration.

   (c) If the condition is a chronic condition (condition #4) or pregnancy, state whether the patient is presently incapacitated and the likely duration and frequency of episodes of incapacity:

---

* The Genetic Information Nondiscrimination Act of 2008 (GINA) prohibits employers and other entities covered by GINA Title II from requesting or requiring genetic information of an individual or family member of the individual, except as specifically allowed by this law. To comply with this law, we are asking that you not provide any genetic information when responding to this request for medical information.

6. (a) If additional treatments will be required for the condition, provide an estimate of the probable number of such treatments: _____. If the patient will be absent from work or other daily activities because of treatment on an intermittent or part-time basis, also provide an estimate of the probable number and interval between such treatments, actual or estimated dates of treatment, if known, and period required for recovery, if any:

   (b) If any of these treatments will be provided by another provider of health services (e.g., physical therapist), please state the nature of the treatments:

   (c) If a regimen of continuing treatment by the patient is required under your supervision, provide a general description of such regimen (e.g., prescription drugs, physical therapy requiring special equipment):

7. (a) If medical leave is required for the employee's absence from work because of the employee's own condition (including absences due to pregnancy or a chronic condition), is the employee unable to perform work of any kind?

   (b) If able to perform some work, is the employee unable to perform any one or more of the essential functions of the employee's job? _____. If yes, please list the essential functions the employee is unable to perform?

   (c) If neither (a) or (b) applies, is it necessary for the employee to be absent from work for treatment?

8. (a) If leave is required to care for a family member of the employee with a serious health condition, does the patient require assistance for basic medical or personal needs or safety, or for transportation?

   (b) If no, would the employee's presence provide psychological comfort to benefit the patient or assist in the patient's recovery?

   (c) If the patient will need care only intermittently or on a part-time basis, please indicate the probable duration of this need?

_____ _____

(Signature of Health Care Provider (Type of Practice)

_____ _____

(Address of Health Care Provider) (Telephone number)

To be completed by the employee needing family leave to care for a family member:

State the care you will provide and an estimate of the period during which care will be provided, including a schedule if leave is to be taken intermittently or if it will be necessary for you to work less than a full schedule:

_____ _____

(Employee signature) (Date)

A "serious health condition" means an illness, injury, impairment, or physical or mental condition that involves one of the following:

1. Hospital Care: Inpatient care (i.e., an overnight stay) in a hospital, hospice or residential care facility, including any period of incapacity or subsequent treatment in connection with or consequent to such inpatient care.

2. Absence Plus Treatment: A period of incapacity of more than three consecutive calendar days (including any subsequent treatment or period of incapacity relating to the same condition) that also involves:

   (a) Treatment[3] two or more times by a health care provider, by a nurse or physician's assistant under the direct supervision of a health care provider, or by a provider of health care services (e.g., physical therapist) under orders of, or on referral by, a health care provider; or
   (b) Treatment by a health care provider on at least one occasion which results in a regiment of continuing treatment[4] under the supervision of a health care provider.

3. Pregnancy: any period of incapacity due to pregnancy or for prenatal care.

4. Chronic Conditions Requiring Treatment: A chronic condition which:

   (a) Requires periodic visits for treatment by a health care provider or by a nurse or physician's assistant under the direct supervision of a health care provider;
   (b) Continues over an extended period of time (including recurring episodes of a single underlying condition); and
   (c) May cause episodic rather than a continuing period of incapacity (e.g., asthma, diabetes, epilepsy, etc.)

5. Permanent/Long Term Conditions Requiring Supervision: A period of incapacity which is permanent or long-term due to a condition for which treatment may not be effective. The employee or family member must be under the continuing supervision of, but need not be receiving active treatment by, a health care provider. Examples include Alzheimer's, a severe stroke, or the terminal stages of a disease.

6. Multiple Treatments (Non-Chronic Conditions): Any period of absence to receive multiple treatments (including any period of recovery therefrom) by a health care provider or by a provider of health care services under orders of, or on referral by, a health care provider, either for restorative surgery after an accident or other injury, or for a condition that would likely result in a period of incapacity of more than three consecutive calendar days in the absence of medical intervention or treatment, such as cancer (chemotherapy, radiation, etc.), severe arthritis (physical therapy), kidney disease (dialysis), etc.

FREQUENTLY ASKED QUESTIONS & ANSWERS REGARDING FMLA

Q: How much leave am I entitled to under the FMLA?

If you are an "eligible" employee, you are entitled to 12 weeks of leave for certain family and medical reasons during a 12-month period.

Q: Who is an "eligible" employee under the FMLA policy?

Employees are eligible to take FMLA leave if they have worked for the School for at least 12 months and have worked at least 1,250 hours over the previous 12 months.

Q: Do the 12 months of service with the School have to be continuous or consecutive?

No. All time worked for the School is counted.

Q: Do the 1,250 hours include paid leave time or other absences from work?

No. The 1,250 hours include only those hours actually worked for the School. Paid leave and unpaid leave, including FMLA, are not counted.

Q: How do I determine if I have worked 1,250 hours in a 12-month period?

Your individual record of hours worked would be used to determine whether 1,250 hours had been worked in the 12 months prior to the commencement of FMLA. As a rule of thumb, the following may be helpful for estimating whether this test for eligibility has been met:

- 24 hours worked in each of the 52 weeks of the year; or
- over 104 hours worked in each of the 12 months of the year; or
- 40 hours worked per week for more than 31 weeks (over seven months) of the year.

Q: How is the 12-month period calculated under FMLA?

The School utilizes a "rolling" 12-month period measured backward from the date an employee uses FMLA.

Q: Is FMLA leave <u>paid</u> time off?

No. The FMLA provides unpaid leave. However, when the leave would otherwise be unpaid, the School requires employees to use accrued paid leave, such as vacation, sick, and personal days, for the FMLA period. When paid leave is substituted for unpaid leave, it is counted against the 12-week FMLA entitlement.

Q: Does workers compensation leave count against an employee's FMLA entitlement?

Yes. FMLA and workers compensation leave run concurrently, provided the reason for the absence is due to a qualifying serious injury or illness.

Q: Does the School count leave taken due to pregnancy complications against the 12 weeks of FMLA for the birth and care of my child?

Yes. Pregnancy disability leave or maternity leave for the birth of a child would be considered qualifying FMLA for a serious health condition and counted in the 12 weeks of leave.

Q: Who is considered an immediate "family member" for purposes of taking FMLA?

An employee's spouse, children (son or daughter) and parents are immediate family members for purposes of FMLA. The term "parent" does not include an "in law." The terms son or daughter do not include individuals age 18 or older unless they are "incapable of self-care" because of mental or physical disability that limits one or more of the "major life activities" as under the Americans with Disabilities Act (ADA).

Q: May I take FMLA for visits to a physical therapist, if my doctor prescribes the therapy?

Yes. FMLA permits you to take leave to receive "continuing treatment by a health care provider," which can include recurring absences for therapy treatments such as those ordered by a doctor for physical therapy after a hospital stay or for treatment of severe arthritis. **However, the School may ask that you schedule these appointments at times that will be least disruptive to the School.**

Q: Do I have to give the School my medical records for leave due to a serious health condition?

No. You do not have to provide medical records. The School will, however, request that for leave taken due to a serious health condition you provide a medical certification confirming that a serious health condition exists.

Q: *May the School require me to return-to-work before I exhaust all my leave time?*

Subject to certain limitations, the School may deny the continuation of FMLA leave due to a serious health condition if you fail to fulfill any obligations to provide supporting medical certification.

Q: *Are there any circumstances in FMLA or reinstatement to my job may be denied?*

Yes. For example, you would not be entitled to FMLA or reinstatement if you would have been laid off or otherwise been terminated had you continued to work during the FMLA period. Moreover, if you give unequivocal notice that you do not intend to return-to-work, you lose their entitlement to FMLA. Also—if you fail to provide any required certification or verification, your request may be denied or reinstatement delayed.

APPENDIX III

Continuation of Health and Dental Insurance

Participants in the health insurance plan sponsored by the Diocese of Manchester who voluntarily resign, are terminated from employment, or otherwise become ineligible for coverage through the plan may elect to continue their participation in the group health plan for a period of time or may elect to purchase coverage through the Health Insurance Marketplace.

Health Insurance Marketplace

Effective January 1, 2014, insurance coverage is available through the Health Insurance Marketplace. A tax credit may be available to lower the monthly premium in the Marketplace. Information about plans, premiums, deductibles, and out-of-pocket costs is available by visiting www.HealthCare.gov. Eligibility for continuation of coverage in the diocesan health plan does not affect eligibility for coverage in the Marketplace.

Continuation of Coverage under the Diocese of Manchester Plan

The Catholic Church is exempt from the federal *Consolidated Omnibus Budget Reconciliation Act of 1985* ("COBRA") and New Hampshire's insurance laws regarding continuation of health coverage. However, the Diocese voluntarily offers continuation of health insurance under certain circumstances for a limited period.

Three groups of people, referred to as beneficiaries, are eligible to elect to continue their coverage: (1) employees or former employees, (2) their spouses and (3) their dependent children. One of several 'qualifying events' must occur to trigger the coverage continuation election as the chart below outlines. Beneficiaries may elect to continue coverage for the maximum coverage period as determined by the beneficiary's status and qualifying event. Beneficiaries must discontinue coverage if other coverage becomes available.

Coverage Continuation Periods

Qualifying Event coverage	*Eligible Beneficiary*	*Maximum*
▪ Job termination ▪ Reduced hours	Employee, spouse, dependent child	18 months
▪ Employee entitled to Medicare ▪ Divorce or legal separation ▪ Death of employee	Spouse, dependent child	36 months
▪ Loss of dependent-child status	Dependent child	36 months

A beneficiary eligible for Social Security Disability Insurance (SSDI) benefits may receive continuation coverage for 29 months.

Continuation coverage ends when any of the following occurs:

- ✓ A beneficiary reaches the last day of maximum coverage.
- ✓ The premiums are not paid on a timely basis.
- ✓ The employer ceases to provide any group health plan.
- ✓ A beneficiary obtains coverage through another employer group health plan.
- ✓ A beneficiary is entitled to Medicare benefits.

The federal *Health Insurance Portability and Accountability Act* ("HIPAA") guarantees that people who have continuous health insurance coverage and meet certain other qualifications cannot be denied insurance even if they have pre-existing conditions. So, if employees forego continuation coverage and create a gap in coverage, they may lose their HIPAA protection when they later decide to purchase insurance.

The process to elect Continuation Coverage:

When an eligible beneficiary has a qualifying event, the person who handles benefits at the parish, Catholic school or diocesan institution where the employee works will notify the administrator within 30 days of an employee's death, job termination, reduced hours of employment, or eligibility for Medicare (under Part A, Part b, or both). In cases of divorce, legal separation or a child's loss of dependent status, *employees* are responsible to notify the person at their workplaces who handles benefits within 60 days of the event.

Once notified, the administrator has 14 days to advise the employee and the employee's family members by first class mail of the option to continue coverage at their own expense. The employee, employee's spouse and dependent child(ren) have 60 days to decide whether to continue coverage. This election period begins from the date the employee's notification is mailed or the date the employee lost coverage, whichever is later (*NB: health insurance continues until the last day of the month in which the employee's resignation, termination or reduction in hours is effective*).

During the election period when employees decide whether to elect to continue their coverage through the diocesan plan(s), employees may initially decide not to continue. As long as the election period has not expired, however, employees may change their minds and revoke the previous declination and coverage would start on the day the declination was revoked. If an employee visits a doctor or other health care provider during the period when the employee initially declined continuation coverage, the employee will not be reimbursed for that claim even if the employee later elects continuation coverage. In this case, continuation coverage is not retroactive to the date the employee lost coverage.

Other considerations:

- Premium payments: employees who elect continuation coverage must pay the first premium within 45 days. The first premium payment is likely to be high as it covers the period *retroactive* to the date coverage ended through the group health plan.
- New workers: newly hired employees will be given an initial general notice about their option to elect continuation coverage in the event of a qualifying event.
- Changing plans: if the Diocese of Manchester offers an open enrollment period to active employees, employees who have elected continuation coverage will be given the option to change plans during this period.
- Moving: if employees move from the health plan's coverage area, they lose their continuation coverage as the diocesan plan is not required to offer a plan in the new area.
- Premium costs: the premiums increase if the costs for the group health plan increase; the plan allows beneficiaries who elect continuation coverage to pay monthly.
- Premium notices: neither the employer nor the administrator is required to send monthly premium notices, so beneficiaries who elect continuation coverage must pay attention to the due dates for premium payments.

APPENDIX IV

ELECTRONIC COMMUNICATIONS POLICY

Introduction

The parishes, schools, and administration of the Diocese of Manchester provide and use a variety of forms of communication and information technologies. The goals in the use of electronic communications media are to spread the Gospel message; to provide information to the faithful so that they may gain a deeper understanding of their faith; to improve communication among diocesan personnel; and to allow access to the wealth of information available on the internet to parish, school, and diocesan personnel. The use of electronic communications media should be viewed as a tool to enhance productivity and further the purposes and goals of the Roman Catholic Church. It is therefore imperative that Church personnel conduct themselves in a responsible, ethical, and professional manner while using electronic communications media. All communication is subject to the boundaries established by our faith tradition, the *Serving Christ, Serving Others* Code of Ministerial Conduct, as well as canon and civil law.

Applicability

This policy applies to all Church personnel. "Church personnel" means all clergy, members of religious institutes, lay employees, and lay volunteers who minister or otherwise provide services to the Diocese of Manchester, its parishes, schools, or institutions.

The policy applies to all "electronic communications media" including, but not limited to, telephone, facsimile, voice mail, computers, tablets, internet and internet access, and electronic mail. The term also includes data storage equipment, digital information devices, personal computers, "smart phones" and similar devices, either owned or reserved for use by the Diocese and its parishes and schools, located on or off diocesan, parish, or school premises.

The term "Church" refers to the Diocese of Manchester and its parishes, schools, institutions, and agencies.

Ownership/No Expectation of Privacy

Electronic communications media purchased or provided by the Church is Church property and subject to inspection. All information created in the course of Church business or ministry and/or produced or carried on Church electronic communications media is likewise Church property and subject to inspection. Church personnel should have no expectation of privacy in the use of electronic communications media when using Church equipment or when conducting Church-related business or ministry. Electronic communications media and any information communicated, received, or stored using such media is the exclusive property of the Church, and although the Church does not regularly monitor electronic communications, they may be monitored, reviewed, retrieved, and stored at any time by Church representatives.

Church personnel must provide their supervisors and/or the network administrator with their passwords for all Church-owned electronic communication media. Church personnel may not share passwords for electronic communications media or secured websites owned or operated by the Church with anyone other than their supervisors and/or the network administrator.

Acceptable Use of Electronic Communications Media

No list of rules for the appropriate use of electronic communications media can be all-inclusive, and this policy does not attempt to articulate all required or proscribed behavior by Church personnel. All communications originating at the Church or using Church-owned equipment must be consistent with the teachings of the Roman Catholic Church, the letter and spirit of the *Serving Christ, Serving Others* Code of Ministerial Conduct, civil and canon law, and the Diocese of Manchester Public Policy Directives.

- *General e-mail and internet use*: During office hours, church personnel are expected to use electronic communications media only for work purposes, except for limited use during break times. Limited personal use of communications is permitted on the express understanding that the Church reserves the right (for its business purposes or as may be required by law) to review Church personnel use and to inspect all material created by or stored on the electronic communications media. Use of the electronic communications media constitutes permission for the Church to monitor communications and to access files that are made on or with these communications tools.

- *Mass Mailings*: Church personnel must obtain prior permission from their supervisor (the pastor, principal, or for diocesan personnel, the Cabinet Secretary), to send mass electronic mailings.

- *Social Networks, Blogs, Wikis, Chat Rooms, Message Boards, Online Comment Sections:* Church personnel are expected to comply with the *Serving Christ, Serving Others* Code of Ministerial Conduct with respect to all electronic communications and use of social networks, blogs, wikis, chat rooms, message boards, twitter, and online comment sections, whether or not employees are using personal or diocesan equipment or are on personal or work time. Church personnel who seek to establish a blog or a social network site (e.g., a Facebook page) for ministry must obtain prior permission from their supervisor (the pastor, principal, or for diocesan employees, the Cabinet Secretary and the Director of Communications) and must comply with the Diocese of Manchester *Guidelines for the Use of Social Networking Sites in Parish Programs* set forth below. Church personnel should not provide information to a "wiki" (a web page, such as Wikipedia or Masstimes.org, that allows visitors to edit content) or online comment sections of newspaper articles, blogs, YouTube video pages, and other forums without prior permission from their supervisor.

- *Linking to Other Websites:* Church websites, including the websites of the Diocese of Manchester and its parishes, schools, and institutions, may provide links only to non-commercial sites that are not in conflict with the teaching of the Roman Catholic Church. All links to other websites must be approved in advance by the pastor, principal, or Director of Communications. Examples of websites to which Church websites may link, include: (1) official Church sites, the Vatican, USCCB, dioceses, and archdioceses; (2) the sites of other parishes, schools, and ministries of or associated with the Diocese of Manchester; and (3) organizations under the oversight of a bishop or religious congregation or that are listed in the Official Catholic Directory.

- *Downloads:* Church personnel must obtain the prior permission of their supervisors or the network administrator before downloading any programs or installing any software on Church equipment. In order to prevent computer viruses from threatening the

network, Church personnel should not open attachments or download content of unknown origin.

- *Electronic Mail:*

    - The use of personal e-mail accounts for communication with minors for ministry or Church-related business is discouraged. Whenever possible, official diocesan, parish, or school email accounts should be used.

    - Any use of electronic communication media through Church accounts for illegal purposes or in support of illegal activities is prohibited.

    - Any use of Church electronic communication media for commercial purposes is prohibited.

    - Any use of Church electronic communication media for partisan political lobbying is prohibited.

    - Church e-mail accounts should be used only by the authorized user(s) of the account for the authorized purpose.

- *Posting Photos, Videos, and Recordings:* Church personnel shall not post online (including on social networking sites) photographs, videos, or recordings without obtaining prior permission for their use. If identifying information about persons depicted in photographs or videos is to be posted, prior written authorization from such persons (or in the case of a minor, the parent or guardian) is required. Such written authorization may, for example, be included in an application or release for a Church-related event or program.

- *Copyright Infringement:* Church personnel must always respect copyrights and trademarks of third parties and their ownership claims in images, text, video and audio material, software, information, and intentions. Church personnel may not copy, use, or transfer materials of others without appropriate authorization.

<u>Guidelines for the Use of Social Networking Sites</u>

"Social Networking Sites" are online websites that are used by groups with a common interest for communication purposes. Social networking sites should be used as a means of effective communication for ministry and education rather than for befriending people or socializing. Every effort must be made to provide a safe and secure environment and to avoid even the appearance of impropriety when using the internet as a ministry tool. Thus, the following guidelines should be kept in mind when considering the use of social networking sites for programs that involve youth under the age of 18. Note: The use of social networking sites is *not recommended* for groups that include students younger than high school age.

- The permission of the pastor, principal, or administrator must be obtained before using a social networking site for a program or ministry.
- Parents must be informed in writing about the use of the social networking site.
- Accounts should be established for the ministry or program; personal accounts should not be used.

- Minors should not be invited to be a “friend.” The minor must make the request.
- The site/group administrator must be an adult. Preferably, there should be two site administrators. The site administrators are considered to work with minors and thus should have completed all safe environment requirements in accordance with diocesan policy.
- Privacy settings may be used in order to protect group members’ privacy, but communication must be transparent and ministry-oriented. Private messaging is strongly discouraged.
- The administrator should pre-approve or regularly monitor all comments and postings. Any inappropriate content should be deleted, and the person who posted it should be contacted and reminded that improper content is not acceptable.
- Rules of conduct should be posted on the site.
- The main purpose of the site should be for general communication about group events rather than for chatting or socializing.
- All information displayed on the site should reflect the Catholic faith.
- Postings should be written as though others will read them. Communications can easily be shared with others for whom they are not intended.
- Whenever possible, copies of communications sent to youth should be maintained. Parents should be copied on communications when possible.
- Photographs may not be “tagged” on social networking sites, such as Facebook.

Further Information

Additional information about the Electronic Communications Policy may be obtained by contacting the Director of Communications for the Diocese of Manchester.

APPENDIX V

RECORDS RETENTION POLICY

2014

DIOCESE OF MANCHESTER

DIOCESE OF MANCHESTER

RECORDS RETENTION POLICY

September 2014

TABLE OF CONTENTS

I. Introduction……... 3

II. Records Retention Overview…… 3
A. Purpose ……. **3**
B. Scope……. **3**
C. Definitions……..... **3**
D. Diocesan Archives……. **4**

III. Records Retention Policy…….. 5
A. Follow Applicable Retention Schedules……... **5**
B. Exception—Litigation Hold…….. **5**
C. Destruction of Records…….. **5**
D. Storage and Preservation of Records…… **5**

IV. Content and Treatment of Specific Types of Files……. 6
A. Records of Clerics and Seminarians……. **6**
B. Lay Employee Records…….. **7**
C. Safe Environment Records……. **8**
D. Electronic Records……..... **9**

V. Digital Imaging ……. 11

VI. Appendix A (Record Retention Schedule)…….. 12

DIOCESE OF MANCHESTER

RECORDS RETENTION POLICY

I. Introduction

The Diocese of Manchester, including all parishes, Catholic schools, and institutions, creates, maintains, and preserves records every day to assist in fulfilling the pastoral mission of the Church in New Hampshire. Records are the principal means of recording the pastoral activity of the Church. Bearing this in mind, the Chancellor has prepared this Records Retention Policy ("Policy") as a normative guide for diocesan administration staff and church personnel in parishes, schools, and other affiliated entities of the Diocese, in determining the manner and length of time for maintaining records. When indicated, records to be destroyed must be done so in a permanent manner. This Policy describes many types of records, and it is important that those responsible for establishing, maintaining and preserving records appreciate the importance of all types of records and consistently follow the guidelines.

This records retention policy[4] was created with reference to the 1983 Code of Canon Law, state and federal statutes, and best practices in record retention. The list of church records included is lengthy, but not definitive. If questions arise regarding records retention issues, please contact the Office of the Chancellor for additional information.

II. Records Retention Overview

A. Purpose. This Records Retention Policy defines which records must be retained for ecclesiastical, canonical, legal or historical purposes, and the retention period for each type of record. Adherence to the established retention schedule is a priority for the Diocese so that (1) vital records are protected and retained; (2) the Diocese reduces its costs associated with maintaining and storing records; (3) the data management and storage operations are enhanced and more efficient.

B. Scope. All records created, received, used, or maintained by the diocese and its parishes, schools, or institutions are the property of the Diocese of Manchester. This Records Retention Policy applies to all church personnel of the Diocese and all parishes, schools, and institutions of the Diocese of Manchester.

C. Definitions.

[4] Some of the provisions in this policy are drawn from the Diocese of Sacramento, *Document Retention Policy* (June 2009) and the Archdiocese of Milwaukee, *Records Retention Guidelines for Parish Records* (1998).

1. "Record" is defined as correspondence, documents (digital or printed), or any other media generated, distributed, or maintained by church personnel in the performance of his or her job duties.

2. "Media" is defined as paper, electronic mail, or electronic/digital storage device (e.g., flash memory device, floppy disk, hard disk, CD-ROM, microfilm, or any other similar data storage medium) used to develop maintain, or transmit church records.

3. "Church personnel" is defined as clergy, religious, seminarians, employees, and volunteers.

D. Diocesan Archives. In the diocesan administration building, there is a permanent archive with three particular sections: general, historical, and confidential. This division of the diocesan archive is delineated in Canons 486-491 of the 1983 Code of Canon Law. An inventory of the records kept in each archive will be maintained at all times in the applicable archive. Documents should not be removed from the archives except for brief periods of time. If a document is removed from these archives, a retrieval record (loan authorization) form must be completed by the archivist and maintained to indicate who has accessed the file, the purpose for access, and the dates the file was loaned and returned.

Access to each section of the diocesan archives is governed by church law. Access to certain documents within some sections of the diocesan archives may be limited as necessary to preserve confidentiality, privacy, and/or the integrity of the records.

1. *General Archive* (Canons 486-488): The records pertaining to the general operations of the diocese are maintained in the *general archive*. The diocesan bishop, vicar general, moderator of the curia, chancellor, archivist, and chancery notaries (secretaries) are provided with access to the *general archives*. Access to other persons in the diocesan *curia* may be granted on a need-to-know basis with permission from the diocesan bishop or the chancellor.

2. *Historical Archive* (Canon 491): The *historical archive* contains records of historical significance to the diocese, parishes, Catholic schools, and institutions. The diocesan bishop, vicar general, moderator of the curia, chancellor, archivist, and chancery notaries (secretaries) are provided with access to the historical archive. Others may be granted permission from the bishop or the chancellor on a need to know basis or for research purposes.

3. *Confidential Canonical Archive* (*Archivum Secretum*, Canons 489-90): The *confidential* or *secret archive* contains files with

documents that are of canonical value or great sensitivity and which need to be kept in conditions of maximum care and security in accordance with the 1983 Code of Canon Law. Access to the *confidential canonical archive* is limited to those authorized under Canon 490, which provides that only the diocesan bishop and certain other people that he designates (e.g., the vicar general and chancellor) may have access.

III. Records Retention Policy

A. Follow Applicable Retention Schedules: Records are to be maintained according to the guidelines established in the Records Retention Schedule (attached as **Appendix A**). Church records older than the retention period should be destroyed in accordance with the destruction directives of this Policy.

B. Exception—Litigation Hold. If church personnel believe, or the Diocese informs them, that records are relevant to current civil or canonical litigation or potential civil or canonical litigation, church personnel must preserve those records until the Chancellor of the Diocese, in consultation with canonical and legal counsel, determines that the records are no longer needed. This exception supersedes any previously or subsequently established destruction schedule for the affected records. If church personnel believe that an exception may apply, or have any question regarding the possible applicability of the exception, church personnel should contact their supervisors or the Chancellor.

C. Destruction of Records. Each department, parish, school, and institution is responsible for the prompt and permanent destruction of all records upon expiration of the scheduled retention period.

1. *Non-confidential documents*: Documents that do not contain any confidential information may be disposed of by recycling or by discarding with other refuse.

2. *Documents bearing confidential information*: Documents that contain any manner of confidential or otherwise private information must be destroyed (shredded) to prevent the danger of confidential information being obtained and misused.

D. Storage and Preservation of Records.

1. *Storage*: Records within the retention period and/or of permanent value should be stored appropriately (e.g., free from damage by insects, climate change, fire, and water). Confidential records and those of permanent value should be stored in a fire resistant and

water resistant vault or cabinet that includes a lock, preferably a combination lock that restricts access to authorized personnel. Care should be taken to store records in appropriately labeled files so that they may be located easily in the future. Records of historical value should not be folded as creases may damage the records. When possible, records of historical value should be preserved on archival paper and stored in acid-free folders.

2. *Computer-generated/digital records:* While most church records exist in hard-copy form, computer-generated church records are also of great value. Church records stored in computer databases may include parish membership and giving (donor) records, financial data, ledgers, personnel records, and payroll information. To ensure the safekeeping of computer-generated/digital church records, the hard drive should be backed up at least weekly, and the back up storage media should be stored separately from the computer itself in a locked fireproof and waterproof vault or cabinet. Information falling into the categories described below should be printed at least annually and stored in hard copy (or should be maintained in accordance with the Digital Imaging provision of this Policy) in accordance with the prescribed retention periods.

IV. Content and Treatment of Specific Types of Files

A. Records of Clerics and Seminarians.

1. *Location of Records*: Certain records pertaining to seminarians, deacons, and priests incardinated in the Diocese of Manchester and assigned by the diocesan bishop are maintained in vaults in the diocesan administration building. Certain records pertaining to clerics who have been granted faculties by the diocesan bishop are maintained in the upper vault, and medical records and other confidential records are maintained in the lower vault (which has limited access). Records pertaining to priests accused of some form of misconduct are maintained in the Confidential Canonical Archive files or by the Office for Ministerial Conduct in accordance with the *Office for Ministerial Conduct File Management Policy*. Records regarding deceased priests are maintained in the lower vault.

2. *Contents of "Personnel Files" for Incardinated Priests, Seminarians, and Permanent Deacons*: Personnel files of priests incardinated in and seminarians of the Diocese of Manchester should contain the following subfiles, where applicable:

- Education/Formation
- Assignments and letters granting faculties
- Correspondence
- Medical records *(Note: Although it is considered part of the personnel file, medical information should be maintained in a file that is physically separate from the personnel file and under lock and key.)*
- Safe environment records[5]
- Legal

Personnel files should not include any correspondence or other documents relating to court cases or alleged violations of the Code of Conduct, and should not contain any investigation materials. Those documents are to be retained separately.

3. *Contents of "Personnel Files" for Non-Incardinated Priests and Permanent Deacons:* The following records regarding priests granted faculties in the Diocese of Manchester (but not incardinated here) and assigned by the Bishop should include, for example:

   - Statement of good standing or letter of suitability from bishop/eparch/provincial
   - Letter granting faculties
   - Assignments (if any)
   - Correspondence
   - Safe environment records

   Personnel files should not include any correspondence or other documents relating to court cases or alleged violations of the Code of Conduct, and should not contain any investigation materials. Those documents are to be retained separately.

4. *Access to Records*: The bishop, vicar general, vicar for clergy, and the chancellor have access to the "personnel files" of priests, seminarians, and permanent deacons. The bishop will designate those other persons who have access. Upon request to the bishop or chancellor, clerics have access to view their own "personnel files," with the exception of recommendations, references, and other documents that are confidential or privileged under civil or canon law.

B. <u>Lay Employee Records.</u>

[5] Safe environment records are defined below.

1. *Contents of Personnel Files for Lay Employees*: A personnel file should be maintained for each active diocesan, parish, school, or diocesan institution employee. Personnel files of employees should contain the following, where applicable:

   - Employee application
   - Resume
   - Eligibility verification form (I-9)[6]
   - W-4 form
   - Employment contract
   - Salary information
   - Benefits information
   - Vacation record
   - Performance evaluations
   - Disciplinary information
   - Medical information *(Note: Although it is considered part of the personnel file, medical information should be maintained in a file that is physically separate from the personnel file and under lock and key.)*
   - Safe environment records

   Personnel files should not include any correspondence or other documents relating to court cases, workers' compensation claims, complaints of discrimination or other illegal conduct, and should not contain any investigation materials. Those documents are to be retained separately.

2. *Access to Records:* These records are *confidential* and should be made available only to diocesan, parish, school, or diocesan institution representatives with a legitimate need to know, unless their disclosure is compelled by legal action. Those with a legitimate need to know may include the pastor of the parish where the employee works, the principal of the school where the employee works, the Cabinet secretary who supervises the employee, and the human resources or personnel director or staff member. They would not include, for example, parish or school advisory board members or clergy or lay staff not responsible for supervision of the employee. The employee has the right to review and request a copy of his or her personnel file, as defined by NH law. Requests should be made in writing and copies of the requests should be stored in the personnel file.

C. <u>Safe Environment Records</u>.

[6] I-9 Forms may be maintained in a separate binder or file specifically designated for I-9 Forms and maintained in a confidential manner.

1. *Definitions:*

   a. "Safe environment records" refers to all paper and electronic documents and communications pertaining to the Diocese of Manchester safe environment screening and training procedures. Safe environment records include, but are not limited to, Screening Forms, Employment Applications, Volunteer Applications, Code and Policy Acknowledgment Forms, criminal records check results, correspondence regarding criminal records checks results, copies of sexual abuse awareness training attendance certificates, and sex offender registry results.

   b. "Active" refers to an employee or volunteer who regularly works with minors (children under the age of 18) at a parish, school, camp, or other diocesan entity.

   c. "Inactive" refers to an employee or volunteer who does not work with minors at a parish, school, camp, or other diocesan entity.

   d. "Works with minors" refers to those employees and volunteers who serve in an *in loco parentis* (in place of parent) capacity or otherwise supervise minors.

2. *Location of Safe Environment Records*

   a. Employee Records: Safe environment records for current parish, school, and camp employees should be stored in an orderly fashion at the diocesan entity either in the employee's personnel file or in a separate file in a locked cabinet or container, with access limited to those with a legitimate need to view them. Applications and paper acknowledgement forms are stored at the diocesan entity, whereas training records, background check results, electronically-signed acknowledgement forms, and sex offender registry results are stored at the Diocese of Manchester Office for Ministerial Conduct and recorded in the Safe Environment Database. Original documents should not be transferred between diocesan entities.

   b. Volunteer Records: Safe environment records for active volunteers who work with minors should be stored in an orderly fashion at the parish, school, or camp in a locked cabinet or container, with access limited to those with a legitimate need to view them. Applications and paper acknowledgement forms are stored at the diocesan entity,

whereas training records, background check results, electronically-signed acknowledgement forms, and sex offender registry results are stored at the Diocese of Manchester Office for Ministerial Conduct and recorded in the Safe Environment Database. Original documents should not be transferred between diocesan entities.

c. Records for former employees and inactive volunteers: Safe environment records for former employees and inactive volunteers should be maintained at the parish, school, camp, or diocesan entity. The records should be kept in a locked cabinet or container with access limited to those with a legitimate need to view them. They should be maintained at the location for seven (7) years following the date when the employee was terminated from service or from when the volunteer discontinued his or her work with minors and will then be transferred to the Diocesan Safe Environment Office for storage.

3. *Archiving of Records:* Employee and volunteer safe environment records that are maintained at the parish, school, or camp will be electronically stored and archived after seven (7) years of inactivity in the Diocese of Manchester. The procedure is as follows:

On a regular basis, the Office for Ministerial Conduct will request from parishes and camps the safe environment files of any employees and volunteers who have been inactive in the Diocese of Manchester for seven (7) or more years and will request from the diocesan Catholic schools the safe environment files of any volunteers who have been inactive for seven (7) or more years (files for school employees must be maintained at the schools due to Department of Education retention laws). A representative of the Office for Ministerial Conduct will collect the files and transfer them to the Office for Ministerial Conduct. The safe environment documents will be electronically scanned into a secure document storage system. The Safe Environment Database status of the archived individual will be changed to “archived” and the record will no longer be accessible except to Office for Ministerial Conduct staff or others with a legitimate need to know.

Should a person whose file has been archived return to ministry with minors, the person will be considered a new volunteer or employee and will be required to complete the safe environment requirements once again.

D. Electronic Records.

a. *"Electronic Record:"* The term electronic record means any record that is created, received, maintained, or stored in diocesan, parish, school, or diocesan institution workstations, central servers, or other electronic devices. Examples include but are not limited to: email, web files, text files, word processing documents, spreadsheets, databases, and other formatted files.

b. *Retention Schedules:* Electronic records must be managed the same as traditional records and in accordance to the Records Retention Schedules (Appendix A) and the policy regarding Litigation Hold (above).

c. *Work-related Files:* Work-related electronic records are records of the diocese, parish, school, and/or diocesan institution and must be retained accordingly. Some records, such as personal or junk email, are not work-related emails and should be deleted from the system immediately.

d. *Archiving Electronic Records:* Computer/email servers are not intended for long-term record retention periods. As a result, all electronic documents required to be maintained should be printed and maintained on paper. Electronic mail in the diocesan offices will be archived for six (6) months, after which the mail will be automatically and permanently deleted, subject to the Litigation Hold provision (above).

V. Digital Imaging

Certain paper records may be maintained in a digital imaging records system and the original paper records destroyed, provided that the original paper records are not required to be maintained under either civil or canon law and the following conditions are met:

- The digital records are complete, accurate, and legible reproductions of the originals;
- The digital records are accessible, available, and readable to all those with a right to access them for as long as they are required to be maintained;
- There are appropriate indexes and other finding aids that will provide access to the information contained in the records;
- Security copies of the digital records and indexes are maintained in secure, off-site storage;
- The original paper records are maintained for a period of six (6) months after converting to digital format for quality control purposes; and
- Authorization for disposal of the original records is obtained from the Chancellor.

APPENDIX A

Record Retention Schedule

		Page
1.	Accounting and Finance	13
2.	Administrative Records (corporation sole/parish)	14
3.	Cemetery Records	16
4.	Confidential Canonical Files (*Archivum Secretum* – Canon 489)	16
5.	Contracts	16
6.	Correspondence and Internal Memoranda	16
7.	Emails	17
8.	Insurance Records	17
9.	Legal Files and Papers	17
10.	Miscellaneous	18
11.	Payroll Records	18
12.	Pension Records/Supporting Employee Data	18
13.	Personnel Records (Clergy)	18
14.	Personnel Records (Lay Employees)	19
15.	Property/Physical Plant Records	20
16.	Publications	21
17.	Sacramental Records	21
18.	Safe Environment Records	22
19.	Safety and Environmental Records	22
20.	School Department/School-Related Records	22
21.	Tax Records	25
22.	Tribunal	25

Record Type	Retention Period
1. Accounting and Finance[7]	
Accounting	
Accounts payable invoices	7 years
Accounts payable ledgers	7 years
Accounts receivable ledgers	7 years
Credit card statements/charge slips	7 years
Tuition collection reports and statements	3 years
Parish collection counts sheets, sealed bag log sheets and fundraising counts sheets	3 years
Invoices and paid bills, major building construction	Permanent
Invoices and paid bills, general accounts	7 years
Cash books	7 years
Cash journals	7 years
Cash journal, receipts on offerings and pledges	7 years
Depreciation records	Permanent
Petty cash vouchers & reconciliation reports	3 years
Receipts	7 years
Mortgage payments & loan statements	7 years
Banking records	
Bank deposits, slips	7 years
Bank statements, reconciliations	7 years
Central Fund statements (savings and loans)	7 years
Cancelled checks, general	7 years
Cancelled checks, important payments	Permanent
Check registers/stubs	7 years

[7] The Diocesan Administration Finance Office also has a Records Retention policy that is consistent with this schedule but addresses specific records.

Record Type	Retention Period
General records	
External audit reports	Permanent
Internal financial review reports	Permanent
Balance sheets, annual	Permanent
Balance sheets, monthly/quarterly	1 year
Budgets, approved/revised	2 years
Financial reports and income statements, annual	Permanent
Financial reports, monthly	1 year
Investment	
Bonds, cancelled	7 years from date of cancellation
Pooled investment reports	7 years
Certificates of deposit, cancelled	3 years after redemption
Letter of credit	7 years
Mortgage records	Permanent
Securities sales	7 years
Stock investments	7 years after sale
Other Financial Records	
General ledger/annual	Permanent
Journals, general and specific funds	Permanent
Journal entry sheets	7 years
Chart of accounts	1 year
Year-end trial balance report	Permanent
Ledgers, subsidiary	7 years
Pledge registers/ledgers	7 years
Permanently restricted gift documents	Permanent
Temporarily restricted gift documents	7 years after meeting restrictions

Record Type		Retention Period
2.	**Administrative Records (corporation sole/parish)**	
	Annual reports to the Bishop (*Status Animarum)*	Permanent
	Annual Financial Reports	Permanent
	Articles of incorporation and bylaws	Permanent
	Bequest and estate records (wills, e.g.)	Permanent
	Board/board committee minutes	Permanent
	Census records	Permanent
	Correspondence, official (regarding diocesan/parish policies, directives)	Permanent
	Correspondence, routine	Review/destroy biannually
	Directives Issued by Decree	Permanent
	Endowment decrees	Permanent
	Finance Council minutes	Permanent
	Historical record (newspaper clippings, photos, etc., regarding history of diocese/parish)	Permanent
	Inventories of property and equipment	Permanent [*or retain until superseded]*
	Leases of any types	7 years after expiration of lease term
	Liturgical ministers' schedules (altar servers, lectors, Eucharistic ministers, etc.)	Retain until superseded
	Mass intention records	2 years
	Office files	Selective retention: review and retain only those that document diocesan/parish administration and official activity
	Organizational records for diocese/parish (minutes, correspondence, publications, etc.)	Permanent
	Pastoral council constitutions	Retain until superseded
	Pastoral council minutes	Permanent
	Priest personnel board minutes	Permanent

Record Type		Retention Period
	Photographs (relating to diocesan/parish history)	Permanent
	Policy statements, policy manuals, employee handbooks	Permanent
	Religious education reports	Permanent
	Rosters of parishioners/parish directories	Permanent
	Wills, testaments, codicils	Permanent
3.	**Cemetery Records**	
	Annual report	Permanent
	Board minutes	Permanent
	Burial cards/records (record of the interred's name, date of burial, and related information)	Permanent
	Burial licenses	Permanent
	Correspondence	Selective retention (retain if record has historical, legal or fiscal value)
	General ledger	Permanent
	Perpetual care records	Permanent
	Financial statements (income statement and balance sheet)	Permanent
	Maps of lots/burials	Permanent
4.	**Confidential Canonical Files** ***(Archivum Secretum – Canon 489)***	
	All files	Retain for period prescribed by the Code of Canon Law
5.	**Contracts**	
	Contracts and related records	7 years after final performance under the contract
6.	**Correspondence and Internal Memoranda**	
	Correspondence or memoranda related to documents enumerated in this Schedule	Same time period as specified for the underlying record

Record Type		Retention Period
	Correspondence or memoranda having no significant or lasting consequences (such as routine letters or notes, letters or memoranda for which no acknowledgement or follow up are necessary)	1 year
	Correspondence or memoranda pertaining to non-routine matters, or having lasting or significant consequences (such as letters explaining diocesan policy)	5 years
7.	**Emails**	
	Emails stored on the server	Six (6) months from date of creation of the email message (subject to longer period as directed by Bishop for compelling reason, including, but not limited to, need to preserve records for longer period due to pending litigation)
	Emails containing material that falls within one of the longer retention periods in this policy	Print email and retain for period specified in this policy
	Ephemeral Correspondence (personal email, requests for recommendations or review, email related to day-to-day operations and ministry)	Retain until read, then delete
8.	**Insurance Records**	
Policies		
	Insurance policies – active	Permanent
	Insurance policies – cancelled	Permanent
Claims files		
	Workers compensation claims files	20 years after close of matter
	Liability claim	10 years after settlement or last correspondence with claimant
9.	**Legal files and Papers**	

Record Type		Retention Period
	Correspondence, legal	10 years
	Legal opinion/memorandum	10 years
	Real estate claims	21 years
10.	**Miscellaneous**	
	Policies/procedures manuals	Permanent
11.	**Payroll records**	
	Payroll journals	7 years
	Payroll registers, summary schedule of earnings, deductions, and accrued leave	7 years
	Payroll/earnings records (timesheets, payroll reports, payroll deduction authorizations)	7 years after end of employment
12.	**Pension Records/Supporting Employee Data (maintained by Plan Administrator)**	
	Pension records/vesting files	For lifetime of plan
	Retirement benefits records	For lifetime of plan
	Pension payment records	For lifetime of plan
13.	**Personnel Records (Clergy, Religious, Seminarians)**	
Incardinated Clergy and Non-Incardinated Externs and Religious		
	Application for Seminary	Until date of death
	Sacramental Documents	Permanent
	Records concerning fitness for duty	Permanent
	Summary regarding Assignments	Permanent
	Background Screening documents	Permanent
	Wills and Funeral wishes	Permanent
	Statements of good standing from bishop/eparch (if applicable)	Permanent

Record Type	Retention Period
Letter granting faculties	Permanent
Seminary records	Until date of death (or return to lay state)
Correspondence	Until date of death (or return to lay state)
Records regarding complaints, misconduct (if applicable)	Until date of death or ten years after condemnatory sentence, if applicable
Summary of allegations of misconduct and conclusions of investigations (if applicable)	Permanent
Medical Records	Until date of death (or return to lay state)
Seminarians/Permanent Deacon Candidates	
Personnel file (including confidential medical and personal information and canonical/sacramental subfiles)	Until ordination – then maintain and follow schedule for incardinated clergy If not ordained by reason of death of the individual – 7 years If not ordained by reason of voluntary or involuntary departure from the program, documents (or a summary) related to the reasons for the departure from the program are to be maintained permanently. All other materials contained in the personnel file are to be retained for 7 years.
Records of applicants for seminary whose applications were rejected or were withdrawn before enrollment in seminary	2 years after the date on which the application was withdrawn or rejected
14. Personnel Records (Lay Employees)	
General records	
Attendance records (time cards, time sheets)	7 years after end of employment

Record Type	Retention Period
Employee contracts (teachers and principals at diocesan schools, extended day care directors, and certain cemeteries department employees)	7 years after end of employment
Employee salary schedules	7 years after end of employment
Payroll/earnings records (timesheets, master payroll reports, payroll deduction authorizations)	7 years after end of employment
Personnel file	7 years after end of employment
Vacation/sick leave records	7 years after end of employment
Separation records	7 years after end of employment
School employee records	
Any school-employee-specific records (such as credentials, degrees, fingerprinting information, tuberculosis screening, bloodborne pathogen training, catechist certification) that may be contained in the employee's general personnel file	7 years after end of employment
Disability/injury/medical records	
Disability records (confidential)	7 years after return to work, retirement or death
Accident/injury reports	7 years
Employee medical complaints	7 years
Employee medical records (confidential)	7 years from end of employment
Job applicant records	
Application records – individuals not hired	2 years
Job advertisement records	2 years
Tax/eligibility/payroll records	
W-2 forms	7 years from date of filing
W-4 forms	7 years from date of filing

Record Type		Retention Period
	I-9 forms	Retain during employment. After end of employment, maintain either: (1) 3 years from hire date; or (2) 1 year after termination date, whichever is greater.
	1099 forms	7 years from date of filing
15.	**Property/Physical Plant Records**	
	Architectural records, blueprints, building designs, specifications	Retain until property is sold
	Architectural drawings	Retain until property is sold
	Deeds and supporting files	Retain until property is sold
	Mortgage documents	Retain until 3 years after mortgage is paid in full
	Property appraisals	Retain until property is sold
	Real estate surveys/plots, plans	Retain 21 years after property is sold
	Title search papers and certificates	Permanent
16.	**Publications**	
	Anniversary books	Permanent (at least one copy)
	Annual reports to the diocese/parish	Permanent
	Diocesan directories	Permanent
	Magazines, newspapers, newsletters of the diocese/parish or affiliated organizations	Permanent
	Parish directories	Permanent
	Parish bulletins	Permanent
17.	**Sacramental Records**	
	Baptism register	Permanent
	First Communion register	Permanent
	Catechumen register (if in use by the parish)	Permanent

Record Type	Retention Period
Confirmation register	Permanent
Book of the Elect	Permanent
Marriage register	Permanent
Marriage preparation records, Marriage envelopes	Permanent
Sick call register	Permanent
Death register	Permanent
18. Safe Environment Records	
Records concerning ongoing employees and volunteers at parishes, schools, or other diocesan entities	Permanent. Parishes, schools, and other diocesan entities transfer the records to the Diocesan Safe Environment Office 7 years after employment or volunteer services permanently cease.
Records concerning clergy or religious assigned to any parish or diocesan workplace	Permanent.
19. Safety and Environmental Records	
Accident/injury reports	7 years from end of year in which occurrence took place
Environmental test records/reports	Permanent
Hazardous exposure records	Permanent
Toxic substance exposure records	Permanent
Safety Data Sheets (Material Safety Data Sheets)	30 years after discontinuation of the use of the toxic substance
20. School Department/School-Related Records	
Administrative records	
Accreditation files	Permanent

Record Type	Retention Period
Assessment materials (student testing materials such as completed exams, forms, reports, and printed materials related to standardized tests/assessments)	Final reports: Permanent Other materials: retain until superseded
Class lists	Permanent
Class schedules	Retain until superseded by new schedule
Faculty meeting minutes	Retain until next accreditation cycle (or three years, whichever is later)
Field trip forms and permission slips	3 years after date of event/trip
Grade books	Cum file reports: Permanent Yearly grade books: 1 year
Student rosters (including graduation lists)	Permanent
Handbooks (faculty, staff, parent, student)	Retain until updated (archive at least one copy permanently)
Newsletters (to parents, school community)	Retain until next accreditation cycle (or three years, whichever is later)
Parent-Teacher Organization minutes	Permanent
Promotion lists	Retain until superseded
Teacher's attendance register	Permanent
Textbook inventory	Retain until superseded
Yearbooks	Permanent
Student records	
Academic dismissal	Permanent (record in cumulative file)
Accident Reports	5 years
Administration of Medication forms	Retain 1 year after transfer
Application, registration, and enrollment records	Retain until end of current school year

Record Type	Retention Period
Attendance Information: 1. Record of Number of Days Absent and Times Tardy 2. Written Absence and/or Tardy notes, dated and signed by parents. 3. Attendance Registers (daily attendance recorded in legal register provide) 4. Sign-in, sign-out sheets (for Preschool, Extended Care and regular school day)	1. Permanent (reported on cumulative record) 2. Retain until end of current school year then destroy 3. Permanent school file 4. Retain in general school file until end of year then destroy
Behavioral Pattern Reports	Retain in separate file (not in cumulative file); destroy 6 months after cumulative file has been transferred to next school.
Certificate of Eligibility for Nonimmigrant (F-1) Student Status – for Academic and Language Students	Permanent; record in cumulative file
Child Abuse Reporting Record	Retain in a confidential separate school file permanently (*if the Administrator is aware of the Report)
Child Custody Records	Permanent; record in cumulative file. Retain in a confidential separate school file permanently.
Detention (Notice of Detention to parents)	1 year
Discipline data	Retain as long as student is enrolled in school
Emancipated Student	Permanent; retain in cumulative file
Emergency information cards	Retain most current card in general school file, destroy previous cards
Expulsion	Permanent; record in cumulative file

Record Type	Retention Period
Guidance Counselor notes	Retain in separate file (not in cumulative file); destroy 6 months after cumulative file has been transferred to next school
Health record	Forward to receiving school when student transfers/graduates (do not retain a copy of the health record)
Health-related occurrence, record of student	Retain 3 years then destroy
Parental authorizations or prohibitions of student participation in specific programs (not field trip forms)	Retain until end of current school year then destroy
Parental restrictions re: access to directory information or related stipulations	Retain until end of current school year then destroy
Permanent Student Record (cumulative record)	Original must be permanently retained by the sending school; a copy must be transferred by mail to the next school upon written request from parent/legal guardian obtained by the school or district where the student intends to enroll
Permission to walk home or to parent's work location after school	Retain until end of current school year then destroy
Referral of student to public agents or counselors	3 years
Restraining Orders	Retain in file until transfer of student or original is superseded
Sports Participation Forms	3 years after conclusion of season for the sport to which form applies

Record Type	Retention Period
Standardized test results 1. Student record label 2. Copy of student report for tests administered while student attended school	1. Permanent – affix to cumulative file 2. Retain in separate file; destroy 1 year after student has transferred schools
Suspension records	3 years after student leaves school. Retain in separate file (not in cumulative file)
21. Tax Records	
Employment taxes, contributions, and payments, including taxes withheld and FICA	7 years from date of filing
W-2 Forms	7 years from date of filing
W-4 Forms	7 years from date of filing
Form 990	Permanent
State tax exemption certificates (income, excise, property, sales/use etc.)	Permanent
1099 Forms	7 years from date of issuance
Unemployment tax records	7 years from date of filing
22. Tribunal Records	
Judicial cases	Permanent, according to the prescripts of Canon Law
Administrative and Documentary cases	Permanent, according to the prescripts of Canon Law
Marriage Dispensations and Permissions	Permanent, according to the prescripts of Canon Law
Radical Sanations	Permanent, according to the prescripts of Canon Law

APPENDIX VI

DATA SECURITY POLICY

I. OBJECTIVE:

Our objective, in the development and implementation of this comprehensive written information security program ("WISP"), is to create effective administrative, technical and physical safeguards for the protection of certain personal information about employees, parents, students, parishioners and others.[8] This WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting such personal information.
For purposes of this WISP, "personal information" means an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such person: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

II. PURPOSE:

The purpose of this WISP is to:

- Ensure the security and confidentiality of personal information as defined herein;
- Protect against any anticipated threats or hazards to the security or integrity of such personal information;
- Protect against unauthorized access to or use of such personal information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

In designing and implementing this WISP, we have (1) identified reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assessed the likelihood and potential damage of these threats, taking into consideration the amount and sensitivity of the personal information; and (3) evaluated the sufficiency of existing policies, procedures, and other safeguards in place to control risks, including training, employee compliance, and means of detecting system failures. We will regularly monitor the effectiveness of these safeguards. We will re-evaluate each of these elements as needed.

---

[8] This policy is also intended to comply with New Hampshire law (e.g., RSA 359-C:20) and Massachusetts law (e.g., 201 CMR 17.00).

IV. DATA SECURITY COORDINATOR:

We have designated _____ to implement, supervise and maintain this WISP. That designated employee (the "Data Security Coordinator") will be responsible for:

a. Initial implementation of this WISP;
b. Initial and ongoing training of other employees (including temporary and contract employees) who have access to personal information, if any;
c. Regularly evaluating this WISP's safeguards, and recommending and implementing improvements as necessary;
d. Evaluating the ability of each of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, and requiring such third party service providers by contract to implement and maintain appropriate security measures with respect to personal information.
e. Reviewing the scope of the security measures in this WISP periodically, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information.
f. Documenting responsive actions taken in connection with any incident involving a breach of security.
g. Conducting a post-incident review and documenting actions taken in response to the incident to ensure personal information security.
h. In case of a security breach or the loss of control of any personal information,[9] contacting the Chancellor of the Diocese of Manchester for guidance on proper reporting procedures, including but not limited to, reports in accordance with New Hampshire law, RSA 359-C:20, and any other applicable laws.

V. INTERNAL RISKS:

In order to combat internal risks to the security, confidentiality, and integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures will be taken:

- A copy of this WISP must be distributed to each employee.
- Employees with access to personal information will be trained on the provisions of this WISP.
- Disciplinary action will be taken for violations of security provisions of this WISP. Access to electronic records containing personal information will be limited to those persons who are reasonably required to have access to such information to perform their job duties. Access to physical records will be reasonably limited.
- All security measures will be reviewed periodically and whenever there is a material change in our practices that may reasonably implicate the security or integrity of

[9] Examples of a "security breach" or "loss of control" are inadvertently sending a document that includes the social security number of an employee to an unauthorized person or entity and theft of a laptop that contains social security numbers or credit card numbers of employees or donors.

records containing personal information. Appropriate upgrades to the security system will be implemented as needed.

- Former employees must return all records containing personal information, in any form, that may at the time of separation from employment be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
- A former employee's physical and electronic access to personal information as defined in this policy must be blocked. At the time of separation from employment, former employees must surrender all keys, IDs, or access codes or badges, business cards, and the like, that permit access to the premises or personal information. Moreover, former employee's remote electronic access to personal information as defined in this policy must be disabled.
- The passwords used by employees with access to "personal information" as defined in this policy must be changed periodically.
- Employees are encouraged to report any suspicious or unauthorized use of personal information.
- Whenever there is a breach of security, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
- Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.
- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with this WISP's rules for protecting the security of personal information.
- We will develop procedures that ensure that reasonable restrictions upon physical access to records containing personal information are in place, and we will store such records and data in locked facilities, secure storage areas, or locked containers.
- Transport of files containing personal information outside the premises will not be permitted except in cases of need and only with the use of reasonable precautions to ensure the security of the personal information.
- When disposing of records containing personal information, we will redact, burn, pulverize, shred, or cross-shred paper documents so that personal data cannot practicably be read or reconstructed. When disposing of electronic records containing personal information, we will destroy or erase such records so that personal information cannot practicably be read or reconstructed.

VI. EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures will be taken:

- There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.
- There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.
- All computer systems must be monitored periodically to ensure that the security programs are operated in a manner reasonably calculated to prevent unauthorized access to personal information.
- There must be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a location or format that does not compromise the data's security.