CATHOLIC DIOCESE OF SAGINAW

SOCIAL SECURITY NUMBER PRIVACY POLICY

In compliance with the Social Security Number Privacy Act, Act 454 of 2004, (the "Act") the Catholic Diocese of Saginaw ("Employer" or "Diocese") requires all employees who use, are exposed to, or have access to employee or other individuals' social security number(s) ("SSN") to maintain the strictest confidentiality of these numbers and prohibits unlawful disclosure of any SSN. To this end, the Diocese expects all employees to comply with the following requirements of the Act:

1. **Prohibited Uses**. No employee shall intentionally do any of the following with the SSN of another employee or other individual:

   (a) Publicly display more than 4 sequential digits of the SSN, including but not limited to visibly printing more than 4 sequential digits on any identification badge or card, membership card, permit, license, or time records in public view.

   (b) Use all or more than 4 sequential digits of the SSN as the primary account number of the individual, unless it is done pursuant to subsection 3 below.

   (c) Require any individual to transmit more than 4 sequential digits of his/her SSN over the Internet or a computer system or network unless the connection is secure or the transmission is encrypted.

   (d) Require any individual to use or transmit more than 4 sequential digits of his/her SSN to gain access to an Internet website or computer system or network unless the system is secure, the transmission is encrypted, or a password or other unique personal identification number or other authentication device is also required to gain access to the Internet website or computer system or network.

   (e) Include more than 4 sequential digits of the SSN in or on any document or information mailed or otherwise sent to an individual if the SSN is visible on or, without manipulation, from outside of the envelope or packaging.

   (f) Subject to subsection 3 below, include more than 4 sequential digits of a SSN in any document or information sent to any individual or entity unless any of the following apply:

      i. State or federal law, rule, regulation, or court order authorizes, permits or requires the SSN appear in the document;

      ii. The document is sent as part of an application or enrollment process initiated by the individual;

iii. The document is sent to establish, confirm the status of, service, amend, or terminate an account, contract, policy, or employee or health insurance benefit or to confirm the accuracy of a SSN of an individual who has an account, contract, policy, or employee or health insurance benefit;

iv. The document or information is mailed at the request of an individual whose SSN appears in the document or information or is mailed to his/her parent or legal guardian.

v. The document or information is mailed in a manner or for a purpose consistent with the Gramm-Leach-Bliley Act, 15 USC 6801 to 6809; with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Public Law 104-191; or with section 537 or 539 of the Insurance Code of 1956, Act 218 of 1956.

2. **Allowable Uses**. The prohibited uses in section 1 above do not apply to the following situations:

(a) Use of a complete SSN that is authorized or required by state, federal statute, rule, regulation, by court order or rule, or pursuant to legal discovery or process.

(b) Use of a complete SSN as part of a criminal investigation or prosecution when provided to, or received from a Title IV-D Agency, law enforcement agency, court or prosecutor.

3. **No Violation.** It is not a violation of 1(b) above -- Use of more than 4 sequential digits of a SSN for a primary account or 1(f) above -- Use of more than 4 sequential digits when mailing documents or information, to use more than 4 sequential digits of a SSN if the use is for any of the following:

(a) An administrative use in the ordinary course of business, by a person or a vendor or contractor of a person, to do the following:

i. Verify an individual's identity or similar administrative task related to an account, transaction, product, service or employment or any of these being proposed;

ii. Investigate an individual's claim, credit, criminal or driving history, such as in a background or reference check;

iii. Detect, prevent, or deter identity theft or another crime;

iv. Lawfully pursue or enforce an individual's legal rights, such as for tax or employee benefit purposes, collection, an audit, or other investigation;

v. Lawfully investigate, collect or enforce a child or spousal support obligation or tax liability, or

vi. Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or to administer the ownership of shares of stock or other investments.

(b) A use of more than 4 sequential digits of a SSN as a primary account number if:

i. The use began before March 1, 2005;

ii. The use is ongoing, continuous, and in the ordinary course of business. If the use is stopped for any reason, this section will no longer apply.

4. **Authorized Access**. The Diocese will allow access to documents or information that contains SSNs only to those individuals who have a legitimate business purpose to access employee or other individuals' SSNs and who adhere to the requirements of this policy.

5. **Destruction and Disposal**. When the Diocese no longer has a legitimate business purpose for the document or information containing an individual's SSN, the document or information must be properly shredded and disposed of to avoid inadvertent disclosure. Destruction and disposal will occur in conjunction with state, federal and the Diocese's records retention policies and requirements.

6. **Penalty for Violation of This Policy**. Any employee who intentionally violates this policy will be subject to discipline, up to and including discharge for misconduct and may be further subject to criminal and civil fines and penalties, including prosecution.

7. **Security Breach of Personal Information**. In the unlikely event that any employee's personal information is accessed and acquired by any non-employee of the Employer without authorization, the Employer will notify all affected employees in writing as soon as possible. Personal information includes an employee's:

- Name;
- Address;
- Telephone number;
- Driver's license or state personal identification card number;
- Social security number;
- Place of employment;
- Employee identification number;
- Employer or taxpayer identification number;
- Government passport number;
- Health insurance identification number;
- Mother's maiden name;
- Checking account number;

- Savings account number;
- Financial transaction devise account number or the person’s account password;
- Stock or other security certificate or account number;
- Credit card number;
- Vital record; and
- Medical records or information.