Catholic Mutual. . . CARES

DATA PROTECTION POLICY

The Church is constantly evolving and making changes to meet the technical needs and expectations of its parishioners. Dioceses, parishes, and schools are developing their own websites and offering new services online in an effort to keep up with today's society. Some of the newer online ventures being offered by Church websites are fundraising, chat rooms, newsletters, employment applications, bulletin boards, tuition/collection/donations online, etc. Oftentimes, personal information is collected by the Church electronically from individuals, including names, addresses, phone numbers, bank and/or credit card account numbers, incomes, etc. A policy should be in place to properly safeguard diocesan/parish sensitive information as well as the personal information of parishioners, students and employees. The following lists items to consider when developing a policy for data protection.

- Any individual who will have access to sensitive information should have a background check completed.
- Access to this information should be strictly limited to individuals who have a business reason to see it.
- Users should be required to utilize passwords that are at least six characters and contain a combination of letters, numbers, and symbols. Passwords should be changed frequently.
- Password-activated screen savers should be used to lock computers after a period of inactivity.
- Procedures should be in place for the appropriate use and protection of laptops, PDA's, cell phones or other mobile devices. Any sensitive information should be in encrypted files.
- Employees and volunteers must be trained to ensure security, confidentiality, and integrity of sensitive information is maintained such as:
    - Locking file cabinets or doors to rooms where records are kept
    - Not allowing passwords to be shared or posted in work areas
    - Ensuring sensitive information is encrypted when sent electronically

    - Reporting suspicious attempts to obtain sensitive information to supervisors

- Employees should be reminded on a regular basis of policy to keep information secure and confidential.
- Impose and follow through with strict disciplinary measures for policy violations
- Terminated employees or volunteers should have their passwords deactivated immediately
- Know where sensitive information is stored and keep it secure. Remember, only authorized individuals should have access.
    - Storage areas of sensitive paper files should be protected against damage from physical hazards such as fire or floods.
    - Sensitive records should be stored in room or cabinet that is locked when unattended.
    - For sensitive information stored on a server or other computer, it should be password protected by a "strong" password.
    - An inventory should be maintained of all computers and other equipment on which sensitive information may be stored.
    - When transmitting credit card information or other sensitive data, use a Secure Sockets Layer (SSL) or other secure connection to ensure information is protected in transit.
    - When collecting sensitive information online directly from parishioners, make secure transmission automatic.
    - If confidential information must be transmitted by email, the data must be encrypted.
- Ensure disposal of sensitive information is done in a secure manner. All paper records should be shredded in a manner that it cannot be read or reconstructed. Data must be erased when disposing of computers, disks, CD's, hard drives, laptops, cell phones or any other electronic devices containing sensitive information.