Protecting personal information

REQUIRED READING

for employees of the

Catholic Diocese of Lexington

Protecting personal information

Five Common Types of Identity Theft

1) Drivers license
2) Social security
3) Medical
4) Financial
5) Character (criminal)

Not only credit cards!

Protecting personal information

- Today – individuals and employers are being held accountable to protect personal identity information in their possession
- Best solution – is to have layered protection, thorough understanding of vulnerabilities, and be vigilant and cautious with identity information

Employers and individuals are all responsible

Protecting personal information

Identity theft is not an information technology or retail enterprise's problem!

Personal information is often compromised at the workplace through routine activities and by being inattentive to security and sensitivity precautions.

Vigilance from everyone is essential!

Protecting personal information

- Federal and state laws require education and precaution to be emphasized at the workplace
- Liabilities are both civil and criminal
  - Fair and accurate credit transaction act (FACTA)
  - Fair credit reporting act (FCRA)
  - Gramm, Leach, Bliley safeguard rules

There are consequences

Protecting personal information

Precautions are rather simple but require vigilance and adherence

- Do not retain private personal information if it is not necessary
- Secure in locked container with limited access any private personal information
- Never leave documents with private personal information in plain view or unattended
- Do not take any private personal information off the premises of the parish/school
- Never disclose private personal information over the telephone or internet and NEVER without the permission of the individual person

Protecting personal information

Early detection, Early reporting

1) If personal private information has been compromised or a compromise is suspect REPORT IT IMMEDIATELY to the Pastor, Pastoral Life Director, Principal, or the Business Manager
2) SECURE all other personal private information
3) Notification of authorities determined by the Pastor
4) Notify Secretariat for Stewardship, CFO or Controller

Protecting personal information

Start now to prevent compromise situation

1) **TAKE STOCK**: know what personal private information is retained in files and computers
2) **SCALE DOWN**: keep only what is essential
3) **LOCK IT**: under lock and key or combination to protect and limit access
4) **PITCH IT**: properly dispose of personal and private information not needed – crosscut shredder is appropriate
5) **PLAN AHEAD**: know the plan to handle a compromise incident

Diocese of LEXINGTON

Protecting personal information

It is impossible to function and minister today unless we collect and hold some personal private information – names, addresses, Social Security numbers, credit card numbers, driver's license numbers, and a plethora of others – about parishioners, clients, and suppliers.

IF THIS INFORMATION FALLS INTO THE WRONG HANDS, IT COULD PUT THESE PERSONS AT RISK OF IDENTITY THEFT

Protecting personal information

- I _____ acknowledge I am responsible to comply with federal and state laws to protect personal private information that I may come in contact with during the performance of my responsibilities within the Catholic Diocese of Lexington
- Furthermore, I will do my best to maintain vigilance protecting personal private information that is accessed by me in the exercise of my job and ministry. I will guard in confidence the identity information that I handle or am exposed to in the scope of my responsibilities.
- I will promptly report any suspected compromise or actual compromise of personal private information to the Pastor, Pastoral Director, Principal, or Business Manager as soon as possible.

- Signed: _____ Date: _____

Parish/School/Entity _____