6 Golden Rules of Data Privacy Compliance

1. Lock Your Doors

* Install locks on all rooms and cabinets containing person information.
* Use the locks.
* Do not keep the keys in the locks or in plain sight.

1. Lock Your Computers

* Password protect all computers.
* Use strong passwords.

(8 characters: not common words, use letters & numbers)

* Change passwords regularly, at least every 90 days.
* Set computers to require password after a few minutes of non-use.
* Do not keep a copy of passwords in an accessible area.

1. Lock Your Data

* Lock up collection checks and other documents containing personal information.
* Encrypt all personal information sent electronically.
* Maintain up to date firewall and anti-virus protection programs.
* Password protect any thumb drives, CD’s or external hard drives.

1. Securely Dispose of Unneeded Information

* Use a level 3 cross-hatch shredder, securely dispose shreds if possible.

1. Require Vendor Compliance

* You must have a compliance letter from all vendors with access to areas where personal information is kept, even if it’s during business hours and/or in an employee’s presence.

1. Take Responsibility Going Forward

* Identify someone to be in charge of compliance and have that person review data privacy processes and procedures at least yearly.
* Make use all individuals with access to personal information complete Diocesan data privacy training at least yearly.

**Immediately contact the Diocese:**

**Cathi Farr 413-452-0683;** [**c.farr@diospringfield.org**](mailto:c.farr@diospringfield.org) **or**

**Mark Dupont 413-452-0648;** [**m.dupont@diospringfield.org**](mailto:m.dupont@diospringfield.org)

**if there is a suspected breach or violation of the rules surrounding data privacy.**