Data Protection Protocol

Vanessa Caruso

As a supervisor, I handle confidential documents, making it necessary to consider how best to protect the data of my supervisees and their directees. This document demonstrates how I will handle these exchanges in my ministry of supervision.

Email

- I will maintain a password-protected email address -- that only I can access -- for receiving my supervision cases and for communicating with my directees/supervisees.
- With my spiritual direction and Fordham student email, I use Virtu Email Protection - an encryption software to send and receive my confidential email documents.
- I have the confidentiality statement at the bottom of my spiritual direction and student emails:
    - CONFIDENTIALITY NOTICE: The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.
- I will delete supervision documents from my email as soon as I download them, empty my trash, and also have set a quarterly reminder on my calendar to delete any overlooked confidential material.

Electronic Devices (computer, ipad, smart phone)

- I have password protection on any device on which I receive email; make phone calls; or conduct video conferencing with directees/supervisees.
- I have two-step verification to my direction and student email logins.
- I have password-protected accounts -- that I do not share with others -- for things like videoconferencing, calendaring, self-scheduling, mobile phoning.
- I delete electronic or shred any supervision documents I receive immediately following the sessions, except those I bring to supervision (as a student), in which case I will delete/shred after my supervision session on it.

Other Practices

- I insist that supervisees disguise names and identities of their directees both in their written cases and in their conversations with me.

- I have these data protection practices written into my covenant with supervisees:

  I, _____*(supervisee's name)* understand that the preparation and emailing of supervision documents requires attention to confidentiality and data protection. As such I agree to:

  - ➔ Maintain a password-protected email address that only I can access for sending my supervision cases to you and for communicating with my directees.
  - ➔ Disguise the names and identities of all directees both in the written cases I prepare and send to you and in my conversations with you.
  - ➔ Maintain password-protected computer files (or locked physical files) for my own supervision case documents and destroy them at regular intervals.

- I will survey my devices quarterly and delete any confidential files that have escaped my notice.

- I recognize that Canada's PIPEDA - The Personal Information Protection and Electronic Documents Act - differs from HIPAA in that the former applies to all personal data, whether in the healthcare industry or not. In other words, once an organization collects data - regardless of province, type or industry - that organization becomes fully responsible for the protection of that data. Although in most provinces of Canada, the data collected by PIPEDA can be stored abroad, in British Columbia (where I reside) mandates that the data be stored in Canada only.