Canon 9 Recommended Practices and Training

1) Identify which data are considered to be sensitive (private and/or vital to operations).

2) Develop and implement a robust data security plan that includes specific precautions for sensitive data, such as the following.
   a. Limit access privileges strictly to data handlers who "need to know" the information to conduct their official duties and responsibilities.
   b. Review and reauthorize user access privileges on an annual basis.
   c. Limit remote access privileges so that data in a secure location cannot be exported to a site that is not secure (e.g., downloads from a secure database into an Excel or PDF file at home).
   d. Maintain high standards for verifying data requests and data sharing. Due diligence prior to sharing data is more than just identifying who wants the data. Ask questions such as: Why do they want it? How will they use it? Will they destroy it properly? How can proper handling be verified? Will they sign an acceptable use agreement? Note that it is often helpful to have these questions answered in writing.
   e. Mandate password rules that make it difficult for hackers to guess. For example, passwords should be six or more characters in length and include at least one letter and one number, as well as an asterisk, exclamation point, or other special character. Passwords should not be names or words that appear in a dictionary.
   f. Require the use of secure transmission technologies, including secure servers, authentication tools, and encryption algorithms.
   g. Store data securely. This requires appropriate physical security, software security, access security, network security, and related behavioral management security.
   h. Establish and enforce security expectations for portable data storage media, including laptop computers, external hard drives, portable drives, etc.

3) Establish and enforce policies governing the release of student data (both private and directory information) in compliance with FERPA, as well as related state and local privacy laws and regulations.
   a. Train all data handlers to understand their responsibilities with respect to FERPA and other applicable statutes and regulations.
   b. Require written permission from a parent to release non-directory information subject to the exceptions identified in FERPA.

4) Train all data handlers to identify which data are general information and which are sensitive.
   a. Ensure that data handlers understand the expectations and consequences of FERPA, HIPAA, and related state or local privacy laws.
   b. Train individuals based on their access privileges to sensitive data. Non-technical staff with access privileges—such as teachers, administrators, or data clerks—need to understand the data system's security safeguards and how they can follow them. Include discussions about the "why" of security as well as the "how," so that learners can internalize this ethical principle and apply it to their work.