

## Data Handling Best Practices

---

In this document we are going to talk about how to securely handle the information we work with at SDCOE. This applies to SDCOE employees as well as vendors, independent contractors, and affiliates.

“Information” comes in all kinds of forms. It can be paper records, digital texts, graphical images, audio, video, microfilm, and many other formats.

“Handling” includes any activity involving information. Creating, collecting, accessing, viewing, using, storing, transferring, mailing, managing, preserving, disposing, or destroying are all examples of information handling.

In any situation where SDCOE information is being handled, there should be an understanding of the sensitivity level of that information, and what measures may be needed for protection. Here are nine ways in which everyone can be a better guardian of SDCOE information.

### 1. Determine How Much Protection your Information Needs

The protection your information may need depends on an assessment of its **Confidentiality**. Information generally falls into one of three categories:

- Confidential
- Sensitive
- Public

Confidential Information involves a high risk of legal liability, significant financial loss, public distrust or other institutional damage if the data were disclosed.

Examples of confidential information include:

- Data protected by HIPAA (health information)
- Data protected by FERPA (student information including grades, exams, rosters, official correspondence, financial aid, scholarship records, etc.)
- Data protected by Gramm-Leach-Bliley (financial information)
- Data subject to PCI (credit or payment card industry) standards
- Data subject to other Federal or state confidentiality laws

- Passwords and PINs
- Personally Identifiable Information (“PII”)
- Personnel data
- Individually identifiable information created and collected by research projects
- Data subject to non-disclosure agreements
- Audit working papers
- Data protected by attorney/client privilege

Sensitive Information involves a moderate need for protection, or limited risk of financial loss, legal liability, public distrust, or harm if this data were disclosed.

Examples of sensitive information include:

- Audit reports
- Email addresses that are not a public record
- Other grants and contracts (not included above)
- Competitive business information
- System security information such as firewall rules and hardening procedures
- Security incident information

Public Information has no requirement for Confidentiality, and insignificant risk of financial loss, legal liability, public distrust or harm if this data were disclosed.

Examples include:

- Directory information, as defined by the SDCOE policy
- Blogs
- Web pages
- Course offerings
- Annual reports

## **2. Collect Only What is Necessary**

- When collecting data, ensure that only the minimum required amount is taken to fulfill institutional responsibilities.
- Collect Social Security Numbers or other Confidential information only when it is needed to achieve necessary and clearly defined institutional purpose.

- Retain full financial information (electronically or on paper), only if written approval has been obtained from the relevant authority.

### **3. Provide Minimum Necessary Access**

- Limit access to information to those with a legitimate interest (“need to know” or “need to do”) based on their institutional responsibilities.
- Do not allow your SDCOE account to be used by others, and never use anyone else’s login information.
- Only grant information access as authorized by the data owner.
- Ensure all vendor access has been approved.
- Guard against unauthorized viewing of such information displayed on your computer screen, keyboard, or login screen.
- Do not leave information unattended and accessible.
- Do not leave keys or access badges for rooms or file cabinets containing information in areas accessible to unauthorized personnel.
- When printing, photocopying or faxing information, ensure that only authorized personnel will be able to see the output. If these machines retain the last document or several documents in memory, be sure to clear the memory after sensitive documents have been processed. Use a fax cover sheet with a confidentiality statement.
- Respect the confidentiality and privacy of individuals whose records are accessed by observing ethical restrictions that apply to the information accessed and by abiding by all applicable laws and policies with respect to accessing, using, or disclosing information.
- Secure portable devices and portable media devices when unattended (e.g., laptop, PDA, smartphone, etc., and CD’s, DVD’s, floppy disks, USB/Flash/Thumb drives, etc.).

### **4. Disclose Only the Minimum Necessary Information**

- Do not discuss or display information in an environment where it may be viewed or overheard by unauthorized individuals.
- Limit a disclosure to the amount of information reasonably necessary to achieve the purpose of the disclosure.
- Disclose information only when necessary and only to the extent that such disclosure is consistent with SDCOE policy and permitted or required by law.
- Ensure Legal Counsel reviews all subpoenas, search warrants, or other court orders prior to release of information.

- Refer requests for information from media representatives (i.e., reporters, TV news crews, etc.) to the relevant authority.
- Report immediately any potential or suspected breach or compromise of, or unauthorized access to Cybersecurity at 858-298-2211 or [securinginfo@sdcoe.net](mailto:securinginfo@sdcoe.net).

## **5. Safeguard Information in Transit**

- Use secure, encrypted and/or password-protected methods of transmission when sending any Confidential or Sensitive data.
- Encrypt email when sending Confidential or Sensitive information, even to other authorized users.
- Send faxes only when the intended recipient is present.
- Use a confidentiality statement at the beginning or end of e-mails to notify the recipient of confidential content.
- Verify fax numbers prior to transmission.
- Ensure information (including device(s) containing information) is always physically secure when carrying or hand-delivering it to a new location. Remove information from secure locations only with prior approval.
- Access information remotely using only secure methods approved by SDCOE Cybersecurity.
- Accessing and transporting Social Security Numbers with a portable device is NOT appropriate.

## **6. Secure Physical Equipment and Resources**

- Actively “lock” your workstation when you are away from your desk; do not wait for or assume the screen saver will self-activate.
- Place devices that can be used to print information in secure locations.
- Physical protection from theft, loss, or damage must be utilized for mobile devices that can be easily moved such as a PDA, thumb drive, or laptop.
- When evaluating new software or appliances, request a security review of the proposed items by SDCOE Cybersecurity BEFORE purchasing or installing.
- When making a change to a service, system, or business process, consider whether any currently functioning security measures will be disrupted. All changes or modifications to the standard architecture should be documented along with any justifications.
- Immediately contact Cybersecurity if there is a theft of any computer, electronic storage media, portable or personal device containing or that has been used to process SDCOE information.

## **7. Safeguard Information in Storage**

- Employ physical protection for all devices (electronic and non-electronic) used to store data.
- Store Confidential or Sensitive Information in a separate location when possible.
- Always encrypt Confidential and Sensitive Information prior to storage. Encrypting data helps ensure that if an access control is bypassed, the information is still not readily available. A standard and published encryption standard should be used. The encryption method and key strength level must be approved by IT Security.
- Limit custody and access to as few people as possible to enhance accountability. Consider documenting transfers of custody.
- Store data on systems that support access control.
- Retain Social Security numbers and other PII only when required (by a “business-related” purpose).

## **8. Dispose of Information Securely When No Longer Needed**

- When retention requirements have been met, records must be either immediately destroyed or placed in secure locations as described in this section for controlled destruction.
- Review, purge, and shred printed documents regularly (in accordance with published destruction schedules).
- Ensure complete destruction of information on electronic storage media, computers, and portable devices prior to disposal/recycling.

## **9. Stay Informed About Information Risks**

- Attend all required Cybersecurity training provided by SDCOE.
- Always be mindful of the value of SDCOE data.