Resources Used:

- BP 10.6
- BP 22.22
- DW AI Taskforce AI Acceptable Use Guidance
- AI Summit AI Critical Literacies and Culturally Responsive Teaching Guide
- FERPA guide
- Emily Moss AI Syllabus
- ChatGPT to help organize/synthesize

DRAFT

Responsible Technology & AI Use at 4CD: A Guide to Data, Privacy, Policy, and Practice

Navigating Data Privacy, FERPA Compliance, Ethical Technology, and Critical AI Literacies at 4CD

---

1. Introduction: Why This Guide Exists

As employees, you interact with sensitive information every day—from student grades to draft budgets to committee notes. This guide is here to help you:

- Understand district policies around data classification, privacy, and technology use.
- Make informed decisions about storing, sharing, and protecting information.
- Safeguard students, colleagues, and yourself by complying with FERPA and ethical practices for emerging technologies like AI.
- Build critical AI literacies to recognize, evaluate, and responsibly use AI in ways that advance equity, cultural responsiveness, and institutional trust.
- Cultivate a culture of data stewardship and literacy rooted in trust, equity, and shared responsibility.
- Provide education and support on data privacy rules and best practices, honoring employee and student agency through a shared understanding of technology tools and their role in participatory governance.

---

2. Quick Reference: What Counts as “Data” at 4CD?

Not all data is the same, and how you treat it matters. Here is a quick guide to understanding data classification in our district (full policy can be found in BP 22.22):

Confidential Data

- Examples: Student grades, ID numbers, disability documentation, financial aid status.
- Example: Employee information…etc
- How to handle: Store only in approved district systems (Canvas, Colleague, secure drives). Never email unencrypted, post publicly, or copy to personal devices.

Sensitive/Internal Use Only

- Examples: Employee personal information (home address, phone number, sexual orientation, race and ethnicity, etc), student information that is not defined as “directory” under FERPA and BP3013.
- How to handle: May be shared within the college/district community but should not be posted publicly or shared outside approved systems.

Public

- Examples: Class catalog info, published event flyers, press releases, tutorials.
- How to handle: Safe to share broadly, but should still be accurate and up to date.
- What are possible risks?

---

3. District Policy and Guidance Doc Summaries

Business Procedure 10.06 – Acceptable Use of Technology

- Requires that all information be classified and handled according to its sensitivity. Confidential information must be secured, tracked, and only accessed by authorized individuals.
- Key takeaways:
    - Use approved systems (Canvas, district email, secure portals) for storing and sharing sensitive information.
    - Avoid personal accounts (Gmail, Dropbox, etc.) for work data.
    - When unsure, treat information as confidential until you confirm otherwise.
- Example: A faculty member emails a spreadsheet with student ID numbers to a colleague’s personal Gmail. If the Gmail account is hacked, student data is exposed. Better choice: use a secure 4CD email or upload the file to a district-approved system, like Sharepoint.

Business Procedure 22.22 – Data Classification Standard

- Groups data into three categories (Confidential, Internal, Public). Each category has rules for where it can be stored, how it can be sent, and who can see it.
- Key takeaways:
    - Always label and treat student information as Confidential unless explicitly classified otherwise.
    - Check storage and sharing rules before sending files or posting documents.

- Example: You want to share draft minutes from a hiring committee. Ask: Is this “Internal Use” or “Public”? Answer: Internal—share only with the committee or through secure channels, not on a public website.

4CD Artificial Intelligence Acceptable Use Guidance

- Faculty decide how or if generative AI tools (like ChatGPT) can be used in their courses. Students must cite AI use and follow academic integrity rules.
- Key takeaways:
    - Set clear syllabus policies on AI use for your courses.
    - Don’t paste student work that contains personal information into AI tools—these tools may not be secure.
    - Model ethical use by citing AI sources when you use them.
- Example: You paste a student essay into an AI tool to generate grading comments. Risk: you may expose confidential student work. Better choice: use AI to brainstorm discussion prompts or rubric ideas—without entering any student data.

---

4. FERPA Refresher for Faculty & Employees

FERPA (the Family Educational Rights and Privacy Act) protects student education records. FERPA classifies protected information into three categories:

- Educational Information
- Personally Identifiable Information
- Directory Information: information kept about the student that is considered public. This information may be released without the student's written permission. Directory info may include:
    - Student names, addresses, phone numbers, email address, degrees and awards, athletic information
- You cannot share grades, enrollment info, or other identifiable student data with anyone except:
    - The student

    - Authorized district personnel with legitimate educational interest
- Parents or guardians of college students do not have automatic rights to see records unless the student consents.

Common scenarios:

- Parent calls for student grades – You cannot disclose without the student's written consent.
- Student grades posted on a hallway wall – Only OK if anonymized (not tied to student names or IDs)
- Discussing grades with the student via district email – OK, as long as the email is secure.

---

5. AI and Emerging Tech: Safe, Ethical, and Culturally Responsive Use

5.1 District AI Guidance

Faculty decide how or if generative AI tools (like ChatGPT) can be used in their courses. Students must cite AI use and follow academic integrity rules, as defined in the 4CD Student Code of Conduct.

Key takeaways:

- Set clear syllabus policies on AI use for your courses.
- Don't paste student work or personal information into AI tools without their consent—these tools may not be secure.
- Model ethical use by citing AI sources when you use them and disclosing your own use of AI to your students.

5.2 Critical AI Literacies for 4CD Employees

Building AI literacy means not only knowing how to use AI, but also understanding its risks, biases, and cultural impacts. At the 4CD AI Summit, we created 4 primary categories for navigating AI critical literacy:

Know & Understand

- What AI is, who makes it, and how it works.
- Types, tools, and applications of AI (chatbots, image generators, etc.).

- AI's historical and social context—recognizing bias, power dynamics, and that AI is never neutral.
  Data training practices and the ethics of consent, privacy, and inclusion.

Use, Apply, Create

- Choose AI tools intentionally and craft effective, context-aware prompts.
- Generate or revise content ethically, respecting originality, copyright, and authorship.
- Integrate AI thoughtfully, balancing opportunities with risks (bias, errors, surveillance).

Evaluate

- Check AI outputs for accuracy, bias, and missing perspectives.
- Assess AI's social impact on equity, justice, cultural representation, and climate.
- Examine whose voices are represented or excluded in AI training data.

Reflect

- Consider AI's impact on your teaching, learning, and creativity.
- Decide when *not* to use AI, especially when it risks privacy, authenticity, or agency.

Attributions: Emily Moss AI Syllabus sabbatical project

5.3 Culturally Responsive AI Practices

AI use should align with culturally responsive teaching and learning:

- **Empower student voice and agency** — co-create projects that reflect diverse cultural knowledge.
- **Build authentic community** — design AI-related activities that encourage peer collaboration and respect for lived experiences.
- **Ensure equitable access** — provide clear guidance and alternative pathways for students who may face barriers to AI use.
  Center diverse perspectives — integrate cultural narratives, decolonized content, and varied assessment methods.
- **Reflect on power dynamics** — acknowledge that educators and institutions hold power in shaping how AI is used and whose voices it amplifies.

---

6. Everyday Guiding Questions

Before you send, upload, or share information, ask yourself:

1. What type of data am I handling (Confidential, Internal, Public)?
2. Do I have student consent to share this?
3. Am I using a secure, district-approved system?
4. Would I be okay if this information accidentally went public?
5. Does this involve an AI tool, and if so, am I following FERPA and data classification protocols?

---

7. Resources and Quick Links

- 4CD Business Procedure 10.06 – Acceptable Technology Use
- 4CD Business Procedure 22.22 – Data Classification Standard
- US Department of Education FERPA Overview
- 4CD AI Summit AI Critical Literacies Guide