Teacher guide - Data privacy & classroom examples

At DACC, it is important that you model appropriate practices for protecting student data and privacy in your daily work with students. Your actions set the standard and reinforce expectations for responsible technology use.

Below are some practical examples you can use to model these practices in your classroom:

- **Screen Locks (Workstations and SIS)**

  As teachers, you are encouraged to acknowledge automatic screen locks as a normal and expected part of a secure environment. These timeouts are enforced through district technology policies, align with industry standards, and provide a natural opportunity to reinforce why unattended devices present a risk.

  Example of modeling this to students: When a workstation locks after 15 minutes, instead of showing frustration, say:
  "My screen just locked for security. In professions like healthcare or IT, leaving a terminal open is a major compliance violation. We practice this here at DACC so it becomes a habit before you move into the workforce."

- **2FA for applications (Microsoft, Google, SIS, LMS).**

  As teachers, you are encouraged to consistently model the use of multi-factor authentication (2FA) across all district systems. 2FA is enforced for all SSO applications and serves as one of the most effective safeguards against unauthorized access. Events like PowerSchool timeouts (after 10 minutes) provide regular, built-in opportunities to demonstrate secure re-authentication during everyday classroom tasks such as taking attendance or entering grades.

  Example of modeling this to students: As a teacher retrieves a phone or hardware key to log back in, they say, "This extra step is called multi-factor authentication. It helps protect sensitive information like grades and personal data. In the workplace, this is one of the most effective ways organizations prevent data breaches."

- **Manually Locking Screens (Workstations)**

  As teachers, you are encouraged to actively model physical and visual security habits within your classroom. While automatic screen locks are in place, manually locking your workstation when stepping away reinforces the importance of protecting sensitive information at all times. This also helps maintain a secure and organized workspace where student data is not left visible.

Example of modeling this to students: Before leaving your workstation or transitioning activities, consider saying something like: *"I'm locking my screen before I step away. Even for a moment, it's important to make sure student information isn't left visible. In the workplace, protecting information like this is part of everyday responsibility."*

- **Secure Printing Hygiene**

  As teachers, you are encouraged to model secure printing practices as part of protecting sensitive information. While print release is enforced through badge scanning or user-specific PINs, it is equally important to demonstrate personal responsibility by ensuring you are the only one retrieving your documents and that nothing is left behind.

  Example of modeling this to students: As you scan your badge or enter your PIN to release a print job, it may be useful to state: *"I authenticate before my documents print so only I can pick them up. Even printed information has to be protected, so I make sure I collect everything and don't leave anything behind. In the workplace, securing information includes what we print, not just what's on the screen."*