Information Security

Private and sensitive information contained within your district data systems should be treated with the utmost care. The data in these systems can be far more valuable to bad actors than banking or credit card numbers. Here are some quick data protection do’s and don’ts:

- DO use system information only for the purpose directly related to performing your job duties or providing education.
- DO access sensitive information only from within secure environments through secure methods.
- DO lock workstations when leaving them unattended.
- DO ensure anti-virus and other security patches are up-to-date.

- DON’T utilize systems for personally identifiable or other sensitive information without reviewing the privacy policy and terms of use.
- DON’T share or discuss sensitive information with those who should not have access to it.
- DON’T leave passwords where others can see or easily find them.
- DON’T click links or download attachments from emails without verifying their authenticity.