In A Nutshell…

Workplace Security

Headlines and concerns about computer hackers, breaches, and viruses highlight the vulnerability of our schools' physical workplace security. Securing information that resides in a computer is just as important as securing the computer itself, as well as information that are stored outside the computer.

How can I secure my workplace?

- ☑ Lock up the office when it is not being attended. Know who is responsible for locking up and securing the office at the end of the work day, especially if the person who normally locks up is away from work.
- ☑ If employee ID cards or badges are issued, make sure they are worn/displayed when on the premises.
- ☑ Make sure front-desk employees and incoming visitors have a clear view of each other to ensure visitors do not wander into unauthorized areas.

> ***Student Emergency Contact Cards Stolen***
>
> *More than 2,000 cards containing personal information of students were stolen from North Miami Beach High School. The cards contained students' emergency contacts, social security numbers, and dates of birth.*
>
> *Source: NBC-Miami, nbcmiami.com, 12/08/11*

- ☑ Store portable storage devices, such as USB sticks (a.k.a. flash drives, thumb drives, jump drives) or CDs, in a secure location when not in use.
- ☑ Lock up laptops in a secure location or with a security cable when leaving it unattended.
- ☑ Retrieve print jobs, copies, or faxes containing confidential or sensitive information immediately.
- ☑ When sending confidential information via fax or hard-copy, make sure the information is clearly marked confidential and ensure that the recipient received the information.
- ☑ Keep hard copies of confidential information in a secure location and out of plain sight when leaving the office or desk unattended. When conducting meetings at a desk or work area, make sure private or confidential files that are not needed for the meeting are put away and out of plain sight.
- ☑ When discussing private or confidential information, make sure the discussion cannot be overheard by others.
- ☑ Properly destroy confidential information that is no longer needed and doesn't need to be stored or archived.
- ☑ Use strong passwords for computers, systems, and accounts. Keep passwords in a secure location and refrain from sharing them with others.
- ☑ When stepping away from the computer, lock the screen or log out.
- ☑ Be careful what is sent in email messages and who the messages are sent to. If confidential information must be sent via email, make sure the message is clearly marked "confidential" and is encrypted. Once a message is sent, it can be easily forwarded to unintended recipients.

Where can I get more information?

Privacy Technical Assistance Center (PTAC)	
PTAC provides resources to educational stakeholders as it relates to data privacy, confidentiality, and security. The website contains technical briefs, white papers, archived webinars and presentations, and checklists.	http://ptac.ed.gov/
Hawaii Board of Education (BOE) Policies	
Relevant policies include: *4610 Student Information and Confidential Records*	http://www.hawaiiboe.net/Policies/Pages/default.aspx

Hawaii State Department of Education ◆ Data Governance Office
P.O. Box 2360 ◆ Honolulu, HI 96804
P: 808.218.6791 ◆ F: 808.440.2859
E: DGO@notes.k12.hi.us

Data Governance Office Websites
Public content
http://www.hawaiipublicschools.org/VisionForSuccess/SchoolDataAndReports/HawaiiDataSources/Pages/Data-Governance.aspx

Employee-related content
https://intranet.hawaiipublicschools.org/offices/dgo

Updated: 3/3/2014