FOCUSED
EDUCATION RESOURCES

Protecting Student Personal Information

WHAT IS STUDENT PERSONAL INFORMATION?

Personal information is any *recorded* information that allows someone to identify a student(s).

- Name, student ID, email address, phone numbers, mailing addresses, photographs, etc.

WHAT ABOUT CONTACT INFORMATION?

- A student's contact information is personal information.
- A teacher's *professional* contact information is not considered personal information.
- A teacher's *personal* contact information is personal information.

WHY PROTECT PERSONAL INFORMATION?

- It's the law in BC. Under FIPPA, school districts must protect all personal information.
- This means making reasonable security arrangements to prevent:
    - Unauthorized access to personal information.
    - Unnecessary collection, use, or disclosure of personal information.
    - Secure disposal of personal information - both electronic and paper copies.

BEST PRACTICES FOR PROTECTING PERSONAL INFORMATION: DO'S & DON'TS

Anywhere

- ✓ Adhere to your district or school guidelines.
- ✓ Minimize the amount of personal information you collect, access or use.
- ✓ Collect only the information you need to complete the task at hand.
- ✓ Always tell people when you collect personal information and tell them how it will be used.
- ✓ Treat all personal information as *confidential.*
- ✓ When required, ensure that *written consent* is obtained from parents or guardians before collecting, using or disclosing students' personal information.
- ✓ Store personal information securely on *encrypted* servers and consider protecting devices with *multi-factor authentication,* at a district level.
- ✓ Talk to IT support about best practices for deleting and destroying personal information.
- ✓ Shred documents that may contain personal information of students or staff.

- ✘ Leave personal information recorded on paper or open on your devices for others to view.
- ✘ Store personal information on USB flash drives or other unencrypted storage devices.
- ✘ Discard or recycle old devices until all personal data is wiped clean.

At School

- ✓ Password protect your devices and lock desks or classrooms when unattended.
- ✓ Collect documents from printers or copiers promptly.
- ✘ Leave papers on your desk or in any place where others might read them.
- ✘ Talk about someone else's personal information in public areas.

At Home

- ✓ Restrict other family members' access to your work laptop, tablet and phone.
- ✓ Conduct online conversations with parents and colleagues in a confidential manner; follow district guidelines for synchronous/asynchronous student communications.
- ✓ Keep documents with personal information in a locked drawer, file cabinet or room.

QUESTIONS?

Refer to your school or district contact with responsibility for privacy related issues.