



RESPONDING TO A SUSPECTED PRIVACY BREACH



PRIVACY is...

...the **right to control** access to your personal information, and the **right to decide** what and how much information you give to others, who it is shared with, and for what purposes.

A PRIVACY BREACH occurs when...

...**personal information** that is collected, used, disclosed, retained or destroyed in a manner **that does not meet privacy requirements** set out in federal and provincial privacy legislation.

Examples of privacy breaches may include, but are not limited to: memory key/jump drive left in a public area containing student data; laptop lost or stolen containing student records on the hard drive; documents containing student or employee personal information left unattended on a photocopier; reports containing employee personal information found unshredded in recycle bins or garbage bins; confidential documents left in public view on an employee's desk or other publicly accessible area.

If you suspect a PRIVACY BREACH has occurred, YOU are encouraged to...

...**notify** your Supervisor immediately, or, in his/her absence, your School Board's Freedom of Information (FOI) Coordinator at *(insert phone number of FOI Coordinator here)*;

...**contain**, if possible, the suspected breach by delaying or stopping the process or activity involving the exposure or mishandling of student or employee personal information.

Following your report of the suspected breach, the FOI Coordinator may contact you to confirm details about the suspected breach.

No further action is required on your part unless further directed by your Supervisor and/or the Board's FOI Coordinator.