

What You Need to Know About Our Media Consent

Privacy has to do with being in control of one's own personal information. Educators play a pivotal role in upholding student privacy rights by cautiously handling electronic records and by keeping parents/guardians fully and frequently informed of how student personal information is used, by accommodating parent/guardian questions & concerns, and obtaining consent when it is required.

Many of our students--the first of the digital generations--have had their entire lives digitally recorded. Electronic records released on the internet are permanent and can easily escape our control. Nobody knows the impact this will have on our kids 15 years from now. What can you do? Act judiciously and model this for students when handling electronic personal information.

Educators can:

When Parents Give Consent on the Media Consent Agreement

- Share or use identifying information in digital format such as images, videos, audio recordings, names, written and creative work -- where it is discoverable or shareable on the World Wide Web
 - E.g., electronic newsletters, class or school websites, blogs, video projects, class and school social media accounts, school and community media publications or broadcast.
- You still need to be prudent with student personal information and make sure there is sound educational rationale for contributing to students' digital footprints.

When Parents *Do Not* Give Consent on the Media Consent Agreement

- You can still use internet and web apps that do not collect or display personal information.
- You can collaborate online with students in the same class, same school, or other schools using board-provisioned platforms (with appropriate privacy settings), e.g., The HUB, Commons, Google Drive
- Display student work in the school, board office, and at educational events in the community such as science fairs
- Display first name and last initial on class lists sent home for valentines, birthday parties
- School pictures, year book pictures

Educators should:

STOP

- Sharing pictures, names, birth dates and other personal information of students on social media, including classroom blogs, with no educational or strategic purpose.
- Using web apps that sell student personal information, collect more than is necessary, target students for behavioural advertising, change their privacy policies without notifying you, retain personal information beyond use of the service, use personal information for reasons other than providing the educational app service.
- Storing student information on personal devices and/or in personal clouds.

START

- Asking yourself, “Would a parent/guardian be surprised by what I am doing?” or “Would parents/guardians expect this to be happening in their children’s classroom?”
- Communicate! Keep parents/guardians informed so they are never surprised.
- Using board-provided storage (GoogleDrive, OneDrive) for information collected on personal devices.
- Reducing student digital footprints by capturing (and showing students how to capture) learning and thinking and work without names and faces when names and faces aren’t necessary.
- Reading the *Parent/Guardian Letter on Personal Information* that is linked to from your school’s webpage. It describes and sets parents/guardian expectations for how school clerical and educators routinely use student personal information.
- Reminding parents/guardians not to post/share photos/videos from school events without consent from other parents/guardians or adult students.

CONTINUE

- Using HWDSB-provided applications and web tools.
- Teaching digital citizenship and safe use of technology.
- Keeping parents/guardians informed of what you are doing with technology.