Introduction

This FAQ is brought to you by the HWDSB Privacy Office to assist students, staff, and their families with maintaining privacy and information security as they learn and work at home. FAQs are grouped thematically to help members of the HWDSB community identify those most relevant to their role:

- Privacy, Cybersecurity, and Technology at Home – General Questions for Everyone
- Questions for Students and their Families
- Questions for Staff
    - Educator-Specific Questions
    - Clinician-Specific Questions

This advice is intended to support setting up a secure online environment and informed consent to online activities, while ensuring HWDSB activities align with policies governing Privacy and Breaches, as well as the *Education Act*, *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the *Personal Health Information Protection Act* (PHIPA). These FAQs reference current best practices and ways of reducing online risk.

Students and their parents/guardians can address questions to their teacher(s) and school principals. Staff are encouraged to reach out to their supervisor. Christi Garneau, Privacy and Information Management Officer, is also available at cgarneau@hwdsb.on.ca and privacy@hwdsb.on.ca to respond to questions and concerns, provide advice, and review documents when requested.

Meet the HWDSB Privacy League!

HWDSB's Privacy League is a team of animal superheroes whose mission is to set the tone for a culture of privacy, security, and information management within the school board community. Watch for helpful tips and ideas from Privacy League members throughout these FAQ!

- **Stewardship Raccoon** is our team leader, helping convey the importance of transparency, communication, and trustworthiness as custodians of personal information entrusted to the HWDSB.
- **Security Bear** reminds us of our responsibilities to detect and manage risks, protect information in our care, and be aware of how our decisions can create or compromise privacy.
- **Access Bunny** represents HWDSB's commitment to making information available to individuals through formal and informal requests.
- **Records Owl** keeps us organized with advice on managing records, especially as we are learning, teaching, and working from home.

FAQ Table of Contents

Keyword Index by Question Number

FAQs are grouped thematically to help members of the HWDSB community with identifying those most relevant to their role. This keyword index can help you identify specific topics that arise across multiple questions and roles.

	Target Audience				
	Everyone	Families	All Staff	Educators	Clinicians
Apps/Software/Programs		19, 20, 24		40	
Clinical/Support Services					46-52
Consent/Permission		17, 24		38, 39, 41	48
Contacting HWDSB	11	23		42	
Copyright		25		43, 44	
Cybersecurity for Kids		13, 14, 15, 18		36	
Email	7, 8			37	
Parental Controls		12, 22			
Passwords	4	13			
Personal Information	9		30, 33	42	47
Phishing/Scams	9, 10				
Privacy Breaches	6		29	39	50, 52
Records Management			30, 31, 32, 35		49
Shared Devices		22	26		
Social Media	11	18		38	
Student Support/Wellness		21		45	51, 52
Technical Support		16	27		
Videoconferencing	6		28, 34	39	46
Wireless Networks	1, 2, 3				

Privacy, Cybersecurity, and Technology at Home – General Questions for Everyone

Creating Secure Networks, Devices, and Accounts

1. **How should I configure my wireless network?**

   Password protect your wireless network and only provide the password to devices you trust. Each wireless modem or router has its own instructions, so check with the service provider or manufacturer for the steps to secure your network. Whenever possible, avoid using the default password because bad actors often already know how to hack these!

2. **Is it safe to use public Wi-Fi networks?**

   Similar to free apps, **free public Wi-Fi networks often trade convenience or cost for privacy**. Please avoid using these because they are not secure. It is possible that service providers and/or other users can monitor your activities and/or access your device. Visiting public places also goes against current physical distancing guidelines and is therefore strongly discouraged.

3. **How can I ensure there is enough wireless bandwidth to allow both learning and working from home?**

   Streaming videos and online gaming can often use up a lot of bandwidth. Most wireless routers and modems allow a "guest network" to be set up to limit certain devices' bandwidth consumption. Check with your service provider or device manufacturer for instructions on how to set this up (don't forget to use a strong password for the guest network). Alternatively, a schedule coordinating your household's online activities including learning, working, and leisure may help alleviate bandwidth concerns.

4. **I keep getting prompted to download or update software. Is this a good idea?**

   Absolutely! Many of these updates address security vulnerabilities and help keep devices and accounts secure. Please avoid delaying these.

5. **How do I create a secure password**?

   Secure passwords or "passphrases" are short phrases that include a combination of UPPER and lower case letters, numbers, and symbols. Choose a passphrase that is easy for you to remember, but hard for others to guess.

   It is best to use a new password for each account. If you have to write down passwords to remember them, store your notes in a secure location away from where others can access them or use a password manager. Never leave a password with your device.

6. Should I cover the camera on my device when I'm not using it?

It is always a good idea to cover the cameras on your laptop, tablet, and cell phone when you're not using them because cybercriminals can hack into devices and turn cameras on without you knowing. Sometimes scammers may trick you into downloading malware that allows them to do this or they may hack in through unsecure wireless networks or unencrypted devices. They may try to use these recordings to blackmail you, such as telling you to give them money or they will post the video on the internet or send it to someone you would not want it to go to. Protect yourself by covering your camera with built in slides, stickers, and powering devices off (not sleep mode) when not in use.

Email Use

7. How can I follow best practices for email security?

Privacy breaches can occur when personal information is sent by email to the wrong recipient. Avoid sending confidential information by email and always double check email addresses before sending!

Best practices include:

⇒ Do not send personal information by email. Use initials in the body of an email if you must identify an individual.
⇒ Double check email addresses to confirm you have the correct recipients before sending.
⇒ Limit attaching personal or confidential information to emails.
⇒ Remember that emails sent within the board between staff are more secure then emails sent outside of the board.
⇒ Limit the use of "Cc" and "reply all" to only those who need to receive your message.
⇒ Log off your computer when not in use.

Please avoid:

⇒ Using names or other confidential information in subject lines.
⇒ Accessing HWDSB email on public or shared computers. Remember to log out and close the web browser when you are finished if you do not have a Board computer to access email from home.
⇒ Printing emails and personal or confidential information at home.
⇒ Forwarding messages from HWDSB email accounts to personal accounts or saving copies on personal devices or personal clouds.

Check out HWDSB's Privacy and Security for Working at Home Sharepoint resource for more information.

8. I need to send a confidential file via email. How should I do this?

Limit attaching personal or confidential information to emails. Staff who must send a confidential document by email, encrypt the file with a strong password. Call the recipient to provide them with the password. Remember that emails sent within the board between staff are more secure then emails sent outside of the board.

⇒ Office document password protection
⇒ Adobe PDF document password protection

9. How can I tell if an email or text message is a scam?

Phishing is an attack that attempts to trick you into taking action. Many of these scams are created by criminals looking to take advantage of victims who are unaware of their tricks.

Does it sound too good (or bad) to be true? Bad actors can often offer rewards (money, gift cards, prizes), threaten punishment (fines, arrest), urgency (time limits), or play on your emotions (make a donation) to convince you to fall for their scams. Scammers often mask fraudulent links and email addresses with official-looking ones to try to trick you into believing they are real. These messages often have poor spelling or grammar and use generic greetings like "dear friend" or "dear customer." Hover over links to determine if these match official ones, if it doesn't it's likely a scam.

HWDSB, government agencies, and banks or other financial institutions will never ask you to click a link and provide personal information in a web-based form or ask you to download something to your computer. Many bad actors are currently trying to play on peoples' fears during times of uncertainty and they are aware of increased online activity due to physical distancing. COVID-19 scams may look like ways of accessing financial and community supports.

Curious to know more about COVID-19 scams? Check out the Canadian Anti-Fraud Centre's COVID-19 Bulletin. You can also sign in to Sharepoint and access HWDSB's Staying Safe Online: COVID-19, Phishing, and Scams resource.

10. I've received a suspicious message. What should I do?

If the message was sent from or received by an HWDSB email address, immediately forward the message to spam@hwdsb.on.ca without replying to the sender, clicking links, or downloading attachments.

But what if it came from someone I know? Common tricks include pretending to be someone you know, an authority figure, or a well-known person to gain a victim's trust. If a suspicious message comes from someone you know, use another way to contact them to confirm it's real before replying, downloading, or clicking links.

You can test your COVID-19 email scam sleuthing skills with this online quiz.

11. Can I use social media to reach someone? E.g., Facebook Messenger, Instagram direct message, Twitter. Are these secure communication tools?

HWDSB's Communications and Community Engagement team monitors messages sent through the central Facebook and Twitter pages. Individual schools and staff will have their own procedures for monitoring and replying to messages received through social media channels. **Social media is not secure and should never be used for sending personal or confidential information.**

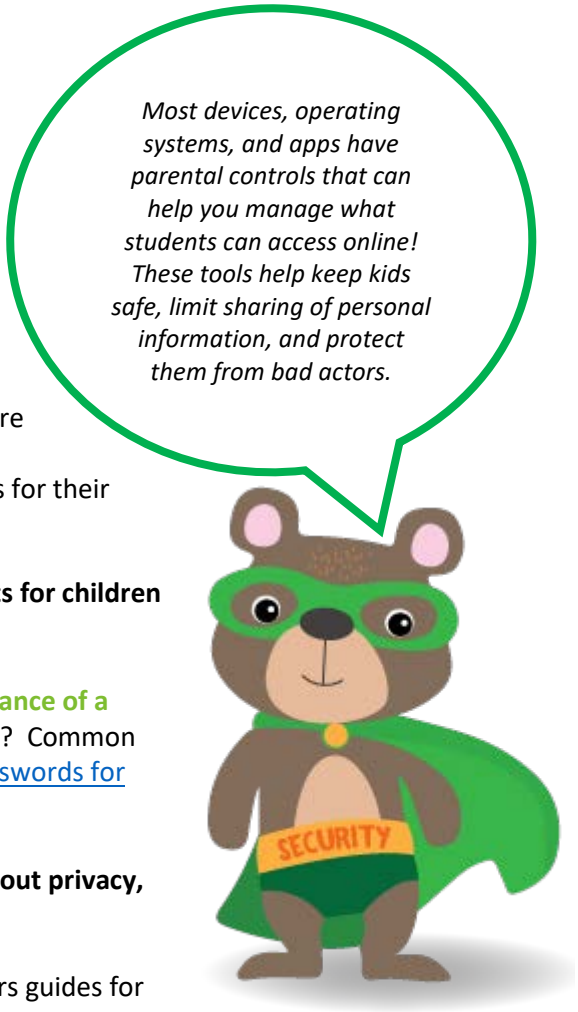
Alternatively, contact information for Elementary Schools and Secondary Schools is available online. You can also reach out to HWDSB directly via the Education Centre. Please be patient and allow staff time to respond to your message as they are also working from home. Mail delivery cannot be guaranteed because buildings are closed.

Staff will not use personal social media accounts for HWDSB activities. This includes sharing classroom updates, corresponding with students and their families, and communicating with staff colleagues. Work-related instant messages and emails sent between staff members on personal accounts are legally HWDSB records. Staff will encourage students and their families to use email, telephone, and the HUB for all HWDSB communications.

Questions for Students and their Families

HWDSB's Supporting and Securing Kids Online at Home is a great introductory resource for families.

Keeping Kids Safe Online



12. **Are parental controls useful for keeping kids safe online?**

    Consider using parental controls to limit internet connectivity to certain times of the day, but be mindful that online tracking and monitoring apps may produce overwhelming amounts of uninformative data so proceed with caution before exploring these. Parents/guardians may want to explore the settings and parental controls built into operating systems, devices, and apps to make informed decisions for their family.

13. **What are good practices for setting up online accounts for children and youth?**

    Choose screen names and logins that minimize the chance of a student being identified online. Looking for some tips? Common Sense Media offers guidance on screen names and passwords for children and youth.

14. **Are there resources I can use to talk to my student about privacy, cybersecurity, and safety online?**

    The Office of the Privacy Commissioner of Canada offers guides for starting conversations with children and youth about topics such privacy, online reputation, sexting and more. Depending on the age of students, not all topics may be relevant or appropriate.

15. **I believe my student may a victim of cyberbullying. What can I do?**

    HWDSB takes concerns about bullying and student safety very seriously. Information is available on the Safe Schools Review Panel website. Parents/guardians can also contact their student's teacher or principal directly with any concerns.

Apps, Programs, and Downloads

16. Who can I contact for technical support?

Students should contact their teacher if the device they are using to learn at home stops functioning or is no longer available to them. Please note that the HWDSB cannot provide technical support for personal devices, but can support families who may need devices to facilitate learning at home

17. What is the age to consent for the apps or programs my student is using?

Although Ontario's *Education Act* sets 18-years-old as the age of consent for educational decisions, many apps/programs based out of the United States use age 13 under the *Children's Online Privacy Protection Rule*. Parents/guardians may wish to speak with their student and/or their teacher if you have questions or concerns about apps they are accessing as part of learning from home.

18. What should I be aware of in terms of social media use?

Parents/guardians can ask: what is our household's definition of privacy? You may want to have a conversation with adults and children about what information should be private, what can be shared, by who, and how. Make decisions together about what to share on social media. Involve students in choosing pictures or videos to post, but respect their wishes if they do not want something shared. Adults may want to start conversations with older children and youth about topics such as privacy, online reputation, sexting and more with these guides from the Office of the Privacy Commissioner of Canada.

The annual Media Consent Agreement also covers sharing of student information, such as photographs or video recordings, via social media. If agreed to, your student's teacher can post photographs, videos, work samples, etc. to classroom social media accounts and these may be publicly accessible. Parents/guardians should speak with their student's teacher or principal if they wish to change their social media consent.

19. I see a lot of advertisements for programs and apps to help my student learn at home. How can I tell if these are Board-approved and safe to download?

Parents/guardians who are unsure whether a program or app is appropriate for their student may find it helpful to consult Common Sense Media for reviews, privacy considerations, and other advice for adults.

Many apps and programs ask students or their parents/guardians to share personal information before they can access them. This may include name, contact information, birthdate, household demographics, and sometimes banking, credit card, or other financial data. Some apps and programs also ask for access to a device's photos, videos, and the ability to record. Proceed with caution before providing any information or granting access to third parties. Remember, free apps often trade personal privacy for cost savings and convenience! Wherever possible, do not share personal information.

Read privacy policies before clicking "yes". Remember, it is always your decision whether to consent to sharing information online!

20. My student wants to use an app or download software that I'm not familiar with. How can I ensure it is safe?

If you're not sure whether a program or app is appropriate for your student, you may find it helpful to consult Common Sense Media for reviews, privacy considerations, and other advice for adults. Also, check out the resources on the Ontario Ministry of Education Learn at home site. And, remember, it is always your decision whether or not to consent to online activities.

Learning at Home

21. How can I set my student up for successful learning online from home?

We are all adjusting to new experiences, including students engaged in distance learning, so it's understandable that families may have to try different strategies to find what works for their household. These tips and tricks may help parents/guardians and students identify strategies to help stay on track:

- ⇒ Choose a central location for family computers or portable device use where adults can supervise what students are doing online. Depending on your home, this could be a kitchen table, office desk, or the family sofa.
- ⇒ Consider whether you can reduce distractions such as toys, other children, or pets to allow students to focus on learning at home.
- ⇒ Establishing a schedule with time limits for online activities and breaks can help make learning at home part of daily routines.

22. We have a shared family device. How can I ensure all the students are able to learn from home?

Families may want to consider setting up a schedule that allows multiple people to share the same device for working and learning. You can also set up multiple user accounts on most devices, allowing each person to sign in and only access their files. Children's accounts should not have administrator privileges so they cannot download software without permission or inadvertently access adults' accounts. HWDSB is also supporting families who need devices to facilitate learning at home. Parents/guardians should contact their student's principal if you require assistance. They can also speak with their student's teacher(s) about strategies to support learning at home.

23. How can I find my student's teacher's contact information?

Contact information for Elementary Schools and Secondary Schools is available online. Parents/guardians can also reach out to HWDSB directly via the Education Centre. Please be patient and allow staff time to respond to messages as they are also working from home. Mail delivery cannot be guaranteed because buildings are closed.

We encourage you to reach out to HWDSB staff by email or phone. Please leave a specific message, including the student's name and a call back number, if you are leaving a voicemail. We will return your call as quickly as we can!

24. My student's teacher is suggesting we download an app or program. Haven't I already consented to my student using apps or programs for learning?

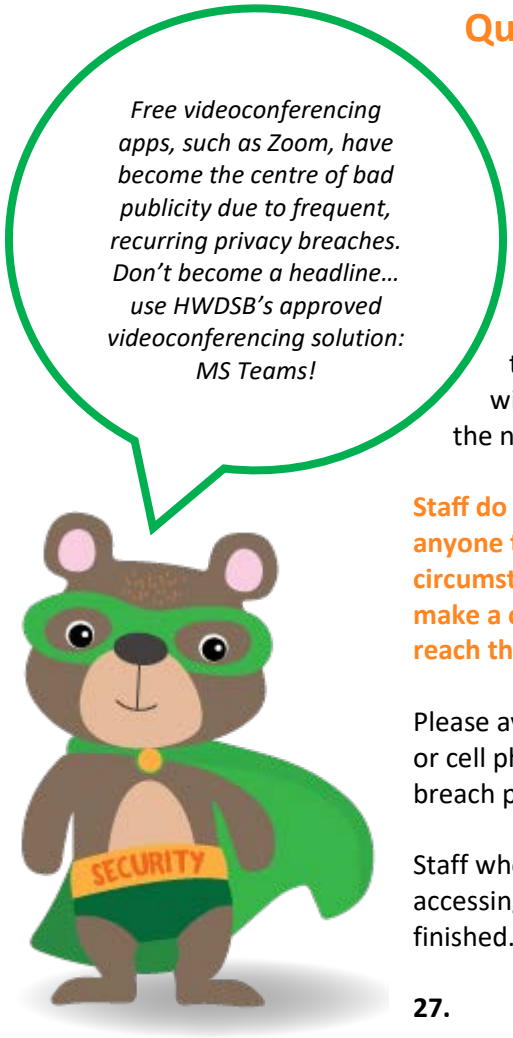
Under the yearly Media Consent Agreement, parents/guardians who provide their consent are agreeing to the sharing of student personal information. **It is HWDSB's responsibility to keep parents/guardians informed about what applications or programs are being used and how student information is shared so that they have an opportunity to ask questions or change their consent.**

25. Are there any copyright considerations I should be aware of when downloading, printing, or sharing material my student receives?

HWDSB abides by all applicable copyright legislation. The Board purchases licenses for online learning materials. Staff are discouraged from suggesting free online resources because these often trade privacy for cost savings. Educators will advise students and their families on any restrictions related to further downloading, printing, or sharing the material they send.

Questions for Staff

Devices, Technical Support, and Software



26. What are some best practices for using personal devices for work?

HWDSB recognizes that many staff members do not have Board-issued cell phones. If staff need to use their personal telephone (cell or land line) to make work-related calls, check with the service provider's instructions for blocking or masking the number before placing a call.

Staff do not have to give out their personal contact information to anyone they would not normally provide it to under regular circumstances. Instead, consider sending an email to set up a time to make a call and ask the student or parent/guardian what number to reach them at.

Please avoid forwarding a Board extension to a shared family land line or cell phone because someone else could answer and accidentally breach privacy or access confidential information.

Staff who do not currently have a dedicated or Board-issued device for accessing email should always log out and close the browser when finished.

27. Who can I contact for technical support?

Staff who have an HWDSB issued device at home that requires service or technical support should place a work order through the Help Desk (eBase). Do not allow someone else to try fixing your HWDSB device. **It can be tempting to ask a well-intentioned friend or family member with technical knowledge to help out, but they may unknowingly compromise the privacy and security of your device.** Please be patient as our technicians have many competing priorities at this time and they will respond to your request as quickly as they can. Staff should notify their principal or supervisor if you do not have an HWDSB device at home or if your recently issued Board device does not work once home.

28. What program does the HWDSB recommend for videoconferencing?

MS Teams is the only videoconferencing platform supported by HWDSB. The Board purchased a license to ensure the privacy, information security, and functionality meets our policies and service standards. Staff must not download or use other videoconferencing software, including Zoom and Facetime, for Board business or on Board devices. Please visit PD Place to sign up for an MS Teams training session to learn more about this platform.

Privacy Breaches

29. I just sent an email to the wrong person. I shared a file with someone who shouldn't have received it. Is this a privacy breach? What should I do?

The Privacy Breach Procedure applies to working from home. Examples of privacy breaches include copying someone on an email they weren't supposed to receive, sending a document to the wrong person, losing a file containing personal or confidential information, sharing contact information without consent, and taking a call or videoconference where others can overhear the discussion. When working from home, family members or housemates may accidentally breach privacy, so staff may want to consider friendly reminders to help protect work information.

Contact Christi Garneau, Privacy and Information Officer, immediately at cgarneau@hwdsb.on.ca or privacy@hwdsb.on.ca or 905.527.5092 x2259 to report unauthorized access to personal or confidential information. We will support you through the breach response procedure.

Workspaces and Record Keeping

30. How can I set my up my workspace to maintain privacy and security?

HWDSB recognizes that although not all staff have a dedicated workspace in their homes, Board policies about Privacy and Breaches still apply. Staff can use these strategies to set up their workspace to maintain privacy and security:

- ⇒ Connect to a password-protected wireless network that only allows access to trusted devices.
- ⇒ Try to take calls and videoconferences from a quiet, private space such as a home office or bedroom to avoid interruptions and someone overhearing confidential, sensitive, or private information.
- ⇒ Avoid printing documents whenever possible. If something must be printed, ensure files are tidied up and stored securely when not in use. Documents that would normally be shredded should be retained until these can be returned to school board facilities for secure destruction.
- ⇒ Be mindful not to overshare staff personal information, such as home phone numbers, with Board contacts who would not normally receive access. Check with telecom service providers for instructions on how to block a number on outgoing calls.
- ⇒ Help keep Board devices secure by reminding family and guests that only staff can use these devices. Lock screens when stepping away (Windows Key + L or Apple Key + L).

Check out HWDSB's Sharepoint resources including Privacy and Security Working at Home for more guidance on setting up your workspace.

31. I normally need to access files from my classroom or office. What can I do from home?

Staff should not remove files containing personal or confidential information from HWDSB facilities without permission from their supervisor. Staff should contact their supervisor directly if they have questions about how they can fulfill their work responsibilities from home.

32. How should I store HWDSB files while at home?

It is best to lock HWDSB files in a secure cabinet, but if staff do not have one, they should please take extra precautions to protect their work materials containing personal or confidential information. Tidy these up when not in use, preferably with a file box, tote, or reusable bag that can be tucked in a discreet area. If necessary, staff can offer a friendly reminder to family members not to disturb their HWDSB items. **Please do not leave HWDSB items unattended in a vehicle at any time.**

33. How do I determine if a file contains personal or confidential information?

Staff need to take additional precautions when working with personal or confidential information from home. Personal information is information that identifies an individual such as name, contact information, date of birth, photos, videos, OEN, education records, human resources files, and health information. Examples of confidential information include sensitive, privileged, or otherwise private Board records such as legal documents, accounting records, drafts of policies and procedures, invoices, procurement files, and others not normally made publicly available. Contact your supervisor or Christi Garneau, Privacy and Information Management Officer at cgarneau@hwdsb.on.ca or privacy@hwdsb.on.ca for advice about handling personal or confidential information.

34. I need to make private phone calls and/or participate in video conferences. How can I do this confidentially?

We all have a responsibility to prevent privacy breaches when working from home. Please be mindful of who might overhear a work phone call or where you place your work files when not in use so those you live with do not accidently access things they shouldn't.

Remember, MS Teams is HWDSB's ONLY approved videoconferencing program. Staff can register for a training session on PD Place. It is best to move to a quiet place at home, away from other people, such as an office or bedroom. It may be helpful to offer a friendly reminder to others at home before taking a private work call and ask not to be interrupted. Although not ideal, staff could also consider taking a call from your parked vehicle if you have one you can access without using shared exits. Keep your mic muted when not speaking in meetings to avoid others in your house from being heard during your meeting. Consider not turning on your camera, or use the background blur function in Teams to prevent colleagues from seeing what is going on behind you.

35. How should I handle documents I would normally discard in the shredder bin at work?

Access and privacy laws governing HWDSB set out very specific requirements for securely destroying documents. Most low-cost shredders sold at big box stores do not meet these legal requirements. **Documents containing personal or confidential information should never be placed in residential garbage or recycling containers.** Staff who do not have access to a cross-cutting shredder at home, should place materials to be shredded in a single, marked file folder or envelope stored with their other HWDSB materials and place these in the shredder bin at their work site when normal business resumes. For safety reasons, please do not burn or find other "creative" ways to destroy documents at home that would normally be shredded.

Any files staff would normally save and store at their workplace should be kept secure at home until HWDSB resumes business as usual in future. Please do not dispose of these.

Educator-Specific Questions

36. How can I encourage my students and their families to follow best practices for privacy and security when learning from home?

Educators are encouraged to refer students and their families to HWDSB's Supporting and Securing Kids at Home resource available on Sharepoint. You are welcome to download this guide and share it with families.

37. What is the best way to email my whole class?

Use the "Bcc" line in Outlook to send an email to students and families without disclosing their email addresses to others in the class. This is important because contact information is legally personal information that cannot be shared without the individual's permission.

38. I want to use social media to keep connected with my students. Is this okay? What do I need to think about first?

Social media can be a great way to connect with students and their families in ways that respect physical distancing guidelines. Expectations about privacy, professionalism, and consent extend to social media and staff must be mindful of this before sharing personal or professional information. Use the same guidelines when working from home as you normally would for your teaching or support staff role. Only students who have a signed Media Consent Agreement can have their photograph, video, work samples, other potentially identifiable information shared via social media. However, ensure the posts are strategic and always try to find ways to post without disclosing student personal information. Remember, every identifiable post you make adds to a student's digital footprint and takes away their right to control their personal information.

If you are taking photographs or recording audio or video from your home for sharing with students, please be mindful of privacy and professionalism when choosing a backdrop. Consider doing this from a shared space in your home such as a kitchen or living room, making sure that no private or confidential information is accidentally captured such as a class list, inbox open on your device, or family/household photographs you wouldn't want shared with your students or colleagues.

You should always have separate social media accounts for HWDSB and personal activities. Although a staff member's personal social media accounts are their own, we as educators and support staff are trusted to lead by example online. The Ontario College of Teachers has issued a Professional Advisory titled Maintaining Professionalism – Use of Electronic Communications and Social Media for its members. Other regulated professionals working within HWDSB may also have guidelines available from their governing bodies. **Please be mindful that personal posts can have professional consequences and that, even with strong privacy settings, social media is never fully secure.**

39. I'm starting to videoconference with my students. I'd like to share a screenshot on our class social media or blog. Am I allowed to do this?

Educators are identifying new ways of helping students keep connected with school communities during these uncertain times; however, educators are discouraged from sharing images or videos of students learning from home because these pose additional privacy concerns beyond what the Media Consent Agreement describes. For example, students may be participating from private spaces in their homes like bedrooms and identifying information like photographs, monogrammed décor, siblings, etc. may be visible. Retrospectively, some families may see this as an invasion of personal privacy or other students may have personal safety concerns as a result. **Parents/guardians who consented to social media sharing at the start of the school year could not reasonably have anticipated current circumstances, so it is not reasonable to automatically extend consent to sharing recordings of students participating in remote learning from home without additional consent.**

Be careful of free apps that sell personal information to advertisers, or worse, scammers! Paid downloads usually have stronger security settings and better data protection, but proceed with caution if these are not HWDSB-approved.

40. What is the difference between free apps/programs and those that charge money and/or that HWDSB provides?

Apps and programs need a way to make money, so they usually trade personal information for access to their sites. This personal information is often sold to or shared with third parties such as advertisers who use the data to market products, or worse to bad actors who use it to try to scam unknowing victims. **Staff should not be implementing new apps or programs without proper approval from their principal and superintendent.**

Many free apps and programs have not invested in the same privacy and security controls that are built into for-purchase software, including those purchased by HWDSB. In addition to the risks noted above, these gaps can lead to breaches and unauthorized access that

puts students, staff, and the HWDSB at risk. There are many cautionary tales in the media of videoconferences being distributed with explicit videos, hackers posing as students on apps to lure victims, and data breaches, so it is best to avoid these in favour of Board-approved software.

41. How can I ensure parents/guardians are properly consenting to students learning online?

Under the yearly Media Consent Agreement, parents/guardians who provide their consent are agreeing to the sharing of student personal information. It is our responsibility as staff to keep parents/guardians informed about what applications or programs are being used and how student information is shared so that they have an opportunity to ask questions or change their consent. You should provide notice to parents/guardians before introducing a new program or app.

Please note that although Ontario's *Education Act* sets 18-years-old as the age of consent for educational decisions, many apps/programs based out of the United States use age 13 under the *Children's Online Privacy Protection Rule*. Consult with Christi Garneau, Privacy and Information Officer, at cgarneau@hwdsb.on.ca, privacy@hwdsb.on.ca or your principal if you need advice on whether to ask for additional consent.

Access rights do not extend to other people's personal information, including birthdates and contact information. These should never be posted online. Sharing without consent is a privacy breach! Always ask permission first.

42. A family has asked for contact information for a classmate's parent/guardian. How should I handle this?

Personal information, including contact information, cannot be shared without permission. If a classmate or their parent/guardian asks you for another student's contact information, let them know you cannot provide this but can reach out to their family and ask their permission to share it. When contacting the parent/guardian be specific about who is requesting their information so they can make an informed decision. If they agree, it is safe to share the contact information. If they decline, everyone needs to respect this decision.

43. I want to share a resource or worksheet with my class. Are there any copyright considerations I need to be aware of?

HWDSB is committed to principles of "Fair Dealing" and abides by all applicable copyright legislation. The Board

purchases licenses for many online learning resources and educators are encouraged to take advantage of these. The Fair Dealing Decision Tool can help you identify what materials can be reproduced. Educators looking to share specialized learning materials should consult with their principal and/or superintendent to confirm proper licensing is secured before digitizing or distributing.

Many open source (free) resources are licenced under Creative Commons, which allows educators to use these under the specific terms like not-for-profit and with attribution to the creator. Be sure to credit creators in accordance with Terms of Use.

44. I would like to read aloud to my students over videoconference or record a video of me reading a favourite classroom story. How can I do this while respecting copyright?

The Read Aloud Canadian Books Program, a partnership between the Association of Canadian Publishers and Access Copyright, allows for a temporary waiver of license fees related to the reading of all or part of select in-print books from participating authors and publishers and sharing a recorded video of the reading. **Please check the list to confirm the title you wish to share is included in the program to avoid inadvertent copyright violations.** If the title is not included in the program, please speak with your principal, teacher-librarian, or library technician before proceeding because additional licensing fees may be required.

Remember to be mindful of your own privacy rights if you are going to record a video from your home, including making sure personal information is not accidently captured, personal spaces are kept private, and no one else appears in the video without their consent.

45. I have concerns about the wellbeing of one of my students. How should I handle this?

It is understandable that many students and their families are experiencing new stressors at this time. HWDSB has resources that support Mental Well-being during COVID available online. Community partners are available to assist with housing, food security, counselling, and other support needs. Please advise your principal of students or families in need to help connect them with these services.

Educators and support staff with enhanced duties to report child welfare concerns are reminded of their legal obligations to contact Family and Children's Services if they believe this is warranted. See the Information and Privacy Commissioner's resource, *Yes, You Can*, on disclosing student personal information to Family and Children's Services.

Clinician-Specific Questions

46. My work includes clinical practice. Are there additional considerations I should be aware of when engaging in telepractice?

"Telepractice" is the term HWDSB is using to describe the therapeutic and support work provided by regulated health professionals, or staff working under their direction, while working and learning at home. **HWDSB clinicians need to ensure their work from home practices meet both Board and regulatory requirements for their profession or that of their supervisor (as applicable).** These staff may need to take additional steps to work securely from home given the sensitivity of their work. HWDSB's staff-oriented Advice for Telepractice resource is available on Sharepoint. Remember, MS Teams is the only Board-approved videoconferencing program and training is available on PD Place. Your supervisor will communicate expectations and additional considerations to you.

47. I've been asked to reach out to parents/guardians to set up a telepractice session with a student. How can I do this confidentially?

Clinicians can use email, text messages, or phone calls to connect with students and/or their parent/guardian; however, these communications should be focused on seeking consent to provide telepractice and scheduling appointments. **Staff should be cautious not to engage in email or text message correspondence that could be construed as clinical work.**

If you are using your HWDSB online calendar that others have access to, please mark appointments as "private" and whenever possible, use a student's initials and avoid including other details of their files. This minimizes the risk of a privacy breach.

48. How can I ensure a student and/or their parent/guardian has properly consented to receiving support at home?

When parents/guardians initially consented to their student receiving support, it was not reasonable for them to predict this would transition to telepractice. As a result,

additional consent is required. Your supervisor will provide you with the revised consent document and procedure that must be completed before engaging in telepractice.

49. How have record-keeping requirements for clinicians changed now that we are providing telepractice from home?

Clinicians and staff working under their direction must continue to abide by HWDSB record-keeping policies as well as those of their discipline's regulatory body. Staff should seek direction from their supervisor about requirements for securing records at home.

50. Have expectations of session confidentiality changed with the transition to telepractice?

As a general rule, expectations of confidentiality remain the same as when clinicians are providing support face-to-face. **Staff must take all steps necessary to ensure they are working from a private space where others cannot see or overhear their work when providing telepractice.** It may be helpful to offer friendly reminders to others in the home that sessions cannot be interrupted. Staff may also want to be mindful of their own privacy when videoconferencing, including avoiding showing private spaces in their homes or blurring other professional boundaries.

HWDSB's Advice for Telepractice resources for staff and families offer additional recommendations to maintain confidentiality and ensure productive sessions. Clinicians are welcome to download the family resource and share it with parents/guardians.

51. What advice can I provide to students and their parent/guardian to help them have a successful telepractice session?

Parents/guardians may appreciate staff advice about how to set their student up for a successful telepractice session. Depending on your discipline and scope of practice, this may include recommending a quiet, private space free from distractions such as toys, siblings, or pets, or possibly a table or desk if working through an exercise together.

52. Many of the students I work with may not have a private space where they can participate in telepractice. How can I support them during this time?

HWDSB recognizes that a students' home environment may pose challenges to successfully engaging in telepractice. The family-oriented Advice for Telepractice guide available on Sharepoint may assist clinicians in helping parents/guardians set their student up for successful sessions. Staff should speak to their supervisor if they have concerns in this regard.