

SECURITY AND PRIVACY CONSIDERATIONS WHEN WORKING REMOTELY

GENERAL PRIVACY FOR REMOTE WORK

As we move to more remote and online services in the coming months, there are several practices which need consideration. Firstly, your district email is the professional tool you should be using. Private email systems such as Gmail or Hotmail should not be used for work related tasks. Secondly, all devices with work related information should be protected through strong passwords. Finally, you need to be mindful of personally identifiable information you collect in your home environment and how you keep that information safe from others who do not have access authorization. The following document from the Office of the Information and Privacy Commissioner of BC provides some excellent guidance and links to resources. <https://www.oipc.bc.ca/guidance-documents/2398>

ZOOM SAFETY AND GENERAL VIDEO CONFERENCE

Zoom has been licensed by the Province of BC for all K-12 Students and Teachers. Recently Zoom has come under scrutiny for its privacy and security with concerns raised about vulnerabilities not being closed quickly enough that would allow hackers to execute malicious activities and access personal data. Acknowledging that no system will ever be 100% secure, we are supporting and recommending the use of the Zoom tool, as has the BC Government. We will however continue to monitor that the vendor is being diligent about security and privacy risks that become exposed. Some important precautions you can take to respect student and parent privacy when using Zoom are:

Zoom Continued...

ZOOM CONTINUED...

- To include a password for all meetings so that you cannot be “Zoombombed” by outside people who somehow get access to your meeting link.
- Request that students turn on a virtual background when using the system (provided their technology can support the feature)
- If a virtual background cannot be used, suggest that the computer or iPad be situated to face a blank wall or private space rather than looking into a bedroom, family room, kitchen or other area of a home that should remain private to the family.
- Teach participants to turn off their microphone and to keep video off when not needed in the learning process.

If you are not comfortable using Zoom, we also offer Microsoft Teams in Office 365 for video conferencing and document collaboration. This is our core system in SD79.

BLOCKING YOUR CALLER ID FROM IPHONE

If you do not want families to have your personal cell phone number, you can block the caller ID. This can be done for a one-time call or more permanently through settings.

<https://www.iphonelife.com/content/how-to-block-caller-id-make-private-call-iphone>

TURN OFF LOCATION TRACKING ON IPHONE

If you have concerns that Apps on your phone are tracking your every move, you may be right! Worse, some apps sell this data to companies who then use it to push hyper-targeted ads to your phone. To help reduce how much and when you are tracked read the following article.

<https://www.macworld.com/article/3327570/how-to-disable-location-tracking-on-your-iphone.html>

Review the following for an excellent security document on general iPhone configuration.

<https://www.fastcompany.com/90254589/use-these-11-critical-iphone-privacy-and-security-settings-right-now>

MASKING STUDENT DATA TO STOP PERSONALLY IDENTIFIABLE INFORMATION FROM BEING SHARED

There are many out of country sites that offer excellent learning value, but may require accounts to be created. Such sites may be used when students do not need to enter personally identifiable information. To do this, teachers can make up a cipher code to create accounts that students may use. For example, instead of using Glen Posey, a teacher might use G3349P as a username. Only the teacher would know the cipher for the code and yet the student can login to a site for math or spelling etc to work on automaticity and fluence skills.

WEB BROWSER SECURITY

Security experts continually evaluate browsers for their privacy and security features. The following article presents recommended browsers to keep you safe. As a district we recommend where possible to use Firefox or Safari.

Web Browser Security Continued...

WEB BROWSER SECURITY CONTINUED

Most Privacy Equipped Browsers

-<https://www.digitaltrends.com/computing/best-browsers-for-privacy/>

BLOCK CROSS SITE TRACKING

Intelligent Tracking Prevention works to prevent what's called cross-site tracking, a feature where a cookie served up by one website can track you across the wider web. Safari, Firefox and Chrome all allow you to turn this feature off. By doing so, you keep more of your web browsing activity private. See the below links for how to make the setting changes in Safari, Firefox and Chrome.

-<https://www.theverge.com/2020/2/12/21124844/apple-mac-safari-privacy-tools-private-network-browser-settings>

-<https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop>

-<https://www.theverge.com/2020/2/11/21126427/google-chrome-privacy-tools-private-network-browser-settings>