Technology Use Best Practices

2017-09-01

Password Protection

Your password is your first line of defense. Use these recommendations to ensure your information is kept safe.

- Choose a strong password (e.g., 8 or more characters with a mix of letters and characters that are hard to guess).
- Stanford University has a Password Quick Guide with excellent details: https://uit.stanford.edu/service/accounts/passwords/quickguide
- Do NOT use commonly used passwords like your birthdate, license plate, children's names, etc. "U0apple$k*n" is an example of a strong password. (Please don't use this example).
- Many of us use multiple passwords and often write them down. Make every effort to avoid doing this. If you must, keep your passwords in a secured location. Password safes like LastPass make this task easier.
- Do not share your password with other users.
- Do not save your password in web forms.
- Passwords should be changed every six months for optimal security. The HPSD network will automatically request a password change after 6 months for staff.

Every Day Computer Protection

If you work with sensitive information, take these steps to ensure passersby do not have access to your system.

- Lock your screen when you leave your desk. In Microsoft Windows, "Windows Key, L" will do this.
- To manually lock your Chromebook, useful if you plan on stepping away from your device for a few minutes, click the padlock icon in the status area menu or hold the power button until the screen flashes and the login screen appears.
- Keep your portable devices (such as thumb drives) in a safe place.
- Turn your computer screen to ensure it is not visible to others.
- If applicable, close and lock your office and work area when you are not present.

Keep your System Updated

Systems that are not kept up to date are susceptible to attack. This includes personally owned electronic devices. Accept automatic updates when you are prompted and restart your computer if requested.

Use Safe Browsing Practices

HPSD computers have a Chrome installed as the default browser. Unless you need to use alternate browsers for compatibility reasons, always use Chrome as your web browser.

- Do not visit unfamiliar or suspicious websites. If you must visit them, do not type any personal information into them.

Avoid Spam

All of us receive plenty of spam and unfortunately, some of us are forced to allow emails into our computer from unknown sources because of our positions.

- If you receive an email that you're not sure of, check with your technical contact before opening it. Alternatively, call (780) 523-3337 and ask for technical support assistance.
- You can reduce the amount of spam you receive by checking your spam filtering settings. Undesired email can easily be blocked or marked as spam in Gmail: https://synergyse.com/shared?app=mail&script=3008

No Phishing

Phishing attacks try to lure you into giving away personal or financial information.

- Never click on links in an email that appear to come from EBay, PayPal or banking sites.
- Make sure you are using the latest Chrome web browser.
- To report phishing abuse, contact Tech Support at 780-523-3337 or support@hpsd.ca

Sensitive Information

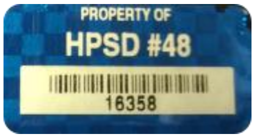
Sensitive information ranges from human resource information, passwords, credit card information, personal identification numbers, to student information.

- Avoid storing sensitive information on your computer if possible.
- If you must store sensitive information on your computer, talk with your technical support staff about ways to ensure it is protected.

Requesting Technical Support

Please use the following options for tech support requests within HPSD.

It is critical that when you run into issue with a Division owned Staff or Student device, you note the Asset ID # of the device in question. Every device in the division with a value in excess of $100 will have a Blue Asset ID tag.



As the division has thousands of devices which the Technology Department actively supports, we need the asset ID # in order to review and troubleshoot your tech concern.

Option A)

Use the handy support request form accessible from the HPSD website (http://www.hpsd.ca) under Support, "Staff Tech Support Form" or simply click this link:

https://docs.google.com/a/hpsd.ca/forms/d/e/1FAIpQLSfu181ETGjVA16F0k80aKENGg7cVHRp8Nind6zDYCW7FXIjcA/viewform

Option B)

Please follow these steps when requesting support:

1) Note the Asset ID# of the HPSD device. This applies to all Staff devices and Student devices.

2) Email your school's tech contact with:

   a. The Asset ID#

   b. The date and the approximate time the issue occurred

   c. A brief description of what the issue is

3) Your Tech Contact will forward this information to the Tech Department via our Ticketing System, Kurious, or via email to suppport@hpsd.ca

4) If your matter is urgent and your Tech Contact is not available, please reach out to the Tech Department directly at support@hpsd.ca or 780-523-3337 with the above information.