

## Questions and Answers

### Updates to PPM 128: Social Media Restrictions on School Networks and Devices

#### **1. What is the definition of social media in the context of this PPM?**

Social media is generally defined as interactive technologies including websites, platforms and applications that facilitate and enable users to create, share, and interact with content, and to connect and communicate with other users or publicly. Examples of social media platforms and apps include Snapchat, Instagram, TikTok, Facebook, X (formerly Twitter), Discord, and similar services that facilitate social interaction and content creation and sharing.

#### **2. Are blogs or any kind of commenting software going to be considered social media?**

The Provincial Code of Conduct requires boards to restrict access to all social media platforms and apps on school networks and school devices. Blogs are different from social media and are not included in the restrictions. However, as a best practice school boards should still apply due diligence on what is allowed and not allowed on its school networks and devices.

#### **3. What measures do school boards need to implement to enforce the restriction of student access to social media platforms and apps on school networks and devices?**

There are different technical ways in which boards can restrict social media platforms and apps on school networks and devices. Approaches may vary from board to board depending on their technology environment, tools at their disposal and their overall approach to the management of traffic on networks and devices.

Every board should assess and determine the best way to meet the requirements of this policy based on their technology environment. Examples of technologies boards can use include SD-WAN to apply restriction policies across the entire school network; SASE (Secure Access Service Edge) to apply restriction policies across all users connecting via the SASE service irrespective of location; locally on devices based on operating system, embedded tools and security tools (e.g. Endpoint Protection Platform).

#### **4. Should Boards use the default social media category in their own firewalls or web filters to implement the social media restrictions?**

Several products may provide pre-defined categories (e.g., social media) to which restriction policies can be applied. However, these are not uniformly defined across different products and manufacturers of network technologies. Also, how social media platforms are defined across manufacturers may vary. Each vendor and platform will have its own definitions and categories. School boards are encouraged to investigate the best approach to applying restrictions based on the technology and tools they have within their environment. This may involve starting with the default social media category on the network/security tool and adjust as needed, or the creation of a custom list or category to which the policy needs to apply.

#### **5. Which social media platform, website or app should the board restrict?**

With technology constantly evolving and the differences in definition for social media across the industry and amongst providers of network and security technologies, every school board should establish and continually manage their restriction list. School boards should consider starting with the platforms and apps that are impacting student participation the most and of greatest concern as it pertains to student well-being. School boards are encouraged to collaborate amongst each other and with the Ministry as these restrictions are applied and evolve over time. Examples of commonly used social media platforms may include Snapchat, Instagram, TikTok, Facebook, X (formerly Twitter), Discord, etc.

#### **6. Are staff included in the social media restrictions outlined in PPM 128?**

Social media platforms are to be restricted on school board networks and board provided devices as a general rule. The ministry understands that some social media platforms may be used in a targeted way for specific learning or operational purposes. School boards can determine exception protocols for the use of social media for pedagogical or work-related purposes.

#### **7. Are smartwatches included as part of the restrictions?**

PPM 128 defines personal mobile device as any personal electronic device that can be used to communicate or to access the Internet, such as a cellphone, tablet, laptop or smartwatch.

All members of the school community must not use personal mobile devices during instructional time except under the following circumstances:

- for educational purposes, as directed by an educator

- for health and medical purposes
- to support special education needs

**8. Will Bring Your Own Device (BYOD) or guest networks be fully blocked?**

BYOD and guest networks must comply with the requirements of PPM 128, including restrictions on social media. Exceptions as stipulated in the PPM also apply to BYOD and guest networks.

**9. How do educators plan to integrate social media platforms into classroom activities while adhering to the policy's guidelines for educational use only?**

Social media platforms can only be accessed by students on school networks and devices for educational purposes, as directed by an educator.

The educator would oversee the use of the platform in the classroom, providing the necessary oversight, guidance, and direction for how the platform would be used for educational purposes.

As set out in the PPM, school boards can determine exception protocols for the use of social media for pedagogical purposes.

**10. Will school board and school communication with parents, guardians and the public be allowed through social media? Will this exception be permitted?**

Yes, school board and school communication with parents, guardians and the public through social media is allowed. PPM 128 states that school boards can determine exception protocols for the use of social media for pedagogical or work-related purposes. This can include exception protocols for the purpose of school boards and schools communicating with parents, guardians, the school community and public through social media.

**11. How will the school boards address concerns regarding privacy and data security in relation to the use of social media platforms and apps for educational purposes under the new policy?**

School boards should always do their due diligence related to security, safety and privacy risks when selecting and using technology in the classroom. This generally involves conducting a privacy and security review of applications to identify risks and appropriate safeguards to protect data and users prior to using the platform or app in the classroom and school.

School boards should also ensure administrators and users of apps and technology are trained on privacy, cyber security, and online safety best practices as well as any related school or board policies (e.g., acceptable use of IT policy).