The Importance of Secure, Safe, and Professional Online Interactions

Pandemic Response
(rev. 11-20)

Connecting virtually presents a way to communicate with staff and families while avoiding potential COVID-19 exposure–but it is not without risk.

With CNC programs engaging in online activities, whether it be internal meetings, professional development, or serving families, it is important to be aware of how your team is interacting.

Security and safety

The swift onset of the pandemic in Canada meant a sudden shift to remote work, often involving new responsibilities, processes, and technology. Some staff may be accessing data through your organization's virtual private networks (VPNs) or cloud computing solutions using their personal devices and home Wi-Fi networks that do not have an adequate level of security. These new arrangements have led to a rapid increase in the number of security threats from cybercriminals who exploit vulnerabilities.

Security breaches on home devices can provide an entryway to an organization's networks and drives that often contain confidential or sensitive data, including information regarding staff and families. These files could be accessed, deleted, stolen, sold, or held for ransom.

According to the Canadian Internet Registration Authority's 2020 Cybersecurity Report:

- Approximately three in ten organizations experienced a sharp increase in the number of attacks suffered since the pandemic began.
- More than 50% of organizations said that they had implemented new cybersecurity protections in response to changes triggered by the pandemic.
- One-quarter of organizations surveyed said that they had experienced a data breach of customer and/or employee data last year._

If cybercriminals gain access to a personal computer, they can also use it to carry out criminal acts, such as spreading malware, illegal information, or illegal images. They can even target the devices of the newcomer families by sending communications that appear to be coming from your CNC program.

In CNC, staff members who have access to children all have completed vulnerable sector screenings. With the move to remote work, there is no organizational oversight over the backgrounds of others in a household. Another threat arises if a device is left unattended, in public view, or is shared by multiple people in a home. Unauthorized individuals may have access to confidential information or be privy to virtual sessions where families, including children, are involved. Identifying objects like pictures in the spaces where calls take place or in unsecured social media accounts–could give clues as to newcomer family members or their location, opening the door to possible physical threats.

Professionalism

Virtual service delivery represents a significant departure from the familiarity of in-person interactions—especially when it comes to connecting with newcomer children.

In order for newcomer families to commit their time, the content of communications has to be relevant and useful. In addition, activities meant to engage children need to be simple enough to implement in a home environment where space and resources may be limited. How you connect with your audience–including the technology you use, the frequency of communications, and your tone–is also essential when building your online presence.

These are important considerations because virtual communications, both between staff and with families, are a reflection of the program's overall quality and professionalism. Your actions in the online domain now will inform the impressions of and confidence in your program when you move back to onsite care–and pave the way for a smoother transition for all involved.

Tips for online interactions

Policies, practices, and standards all have a role to play in keeping both people and information safe and secure while ensuring program professionalism is maintained. It is import to remember the following:

1. Anything you say or do online can be recorded, stored, edited and forwarded without your knowledge.
2. Staff personal information e.g. phone numbers should not be shared with parents. Consider using a company email/ phone number or blocking personal phone numbers.
3. Every interaction with families should be kept professional. The same high standards of personal conduct that are expected in person should be practiced when interacting online.
4. The use of emojis may be misunderstood so it is best to refrain from their use in a professional setting.
5. Strong passwords and 2 step authentication are important tools for online security.
6. Staff should keep their software up to date.
7. Staff should not share their screen when doing a web search during a remote session to prevent the risk of any inappropriate content appearing.
8. Keep track of who is attending online sessions–including staff, children and adults in the home. Remember, in a remote setting there can be other people in the space that can hear and see what is happening.

Click here to download our **Online Interaction Checklist** of things to consider when developing, communicating, and implementing your program's online presence.

Funded by: Immigration, Refugees and Citizenship Canada / Financé par : Immigration, Réfugiés et Citoyenneté Canada