Privacy Practices to Stay Safe While Remote Working

Contents

- Overview
  - Maintain a Secure Connection
  - Keep Sensitive Information Secure
  - Be Extra Careful When Using Personal Devices
- Attachments

Overview

Under these extraordinary circumstances, we are quickly adapting to remote work. In doing so, we continue to promote best practices to protect sensitive data for our employees and students. All employees should try to emulate the same privacy practices in the workplace while in our remote locations. Here are some tips to ensure that sensitive personal or company information stays safe.

Maintain a Secure Connection

- Sign in via Oakland Schools' virtual private network (VPN) before accessing any applications
- Only use Oakland Schools approved teleconference and video conferencing services when meeting with your teams or others. Approved platforms are currently limited to WebEx and Google Meets.

Keep Sensitive Information Secure

- If you are using a laptop, iPad or similar device, never leave it unattended, such as in your vehicle. If you're using a laptop, make sure it is password-protected, locked and secure.
- Remember to protect sensitive information, including personal information about employees, students, customers, vendors, etc. by keeping electronic documents on the Oakland Schools' network, ensuring that any physical copies are kept secure. Documents should be in a locked desk or other locked space others will not have access to. Such documents should not be used as scratch paper.
- Destruction should be consistent with workplace practices. At this time, it is recommended that employee's refrain from printing documents with personally identifiable information unless they have a safe, secure method for destruction which would include cross-cut shredding at home.
- Shred any document that is no longer needed using a shredder with cross-cutting capabilities. If you do not have a shredder, securely store the documents and properly destroy upon your return to the workplace.
- Never leave documents containing personal information unattended unless locked in a secure filing cabinet. If you do not have a file cabinet at home, use a locked room.
- Sensitive personal information or confidential organization information that is transferred in electronic form outside of Oakland Schools' network should be sent via Secure DropBox.
- Always check that recipients and attachments on emails are correct before sending
- Log-out of all work related applications and the Oakland Schools VPN when you are done working for the day.
- If posting or sharing pictures of you working from home on social media sites please ensure your screens and desks are free of any confidential or personal information (employee, student etc.)

Be Extra Careful When Using Personal Devices

- Sign in via Oakland Schools' virtual private network (VPN) before accessing any Oakland Schools applications.
- All work related documents and data should be stored on the Oakland Schools Network or approved application and are not to be retained on the device.
- Employees choosing to use their own personal device(s) must ensure the following protective measures are implemented to protect Oakland Schools data and information including: (1) safeguarding them with strong and unique passwords, and (2) only connecting them to home Wi-Fi networks that are securedwith a strong password and utilize the most up-to-date encryption (WPA2 or WPA3).
- Personal computers must have updated security software installed.

Attachments

File	Modified
Microsoft Word Document Privacy Tips.docx	Apr 10, 2020 by Christopher Usiak
PNG File remote-privacy.png	Apr 10, 2020 by Christopher Usiak

Download All