CREATING OPPORTUNITIES FOR STUDENTS TO KEEP WYOMING STRONG

JILLIAN BALOW
Superintendent of Public Instruction

DICKY SHANOR
Chief of Staff

SHELLEY HAMEL
Chief Academic Officer

KARI EAKINS
Chief Policy Officer

TRENT CARROLL
Chief Operations Officer

CHEYENNE OFFICE
122 W. 25th St. Suite E200
Cheyenne, WY 82002
307-777-7675

RIVERTON OFFICE
320 West Main
Riverton, WY 82501
307-857-9250

ON THE WEB
edu.wyoming.gov
twitter.com/WYOEducation
facebook.com/WYOEducation

WYOMING
DEPARTMENT OF EDUCATION

INFORMATION MANAGEMENT DISASTER READINESS GUIDELINES

This is a collection of ideas, tools, and best practices for districts to consider for scenarios where remote work may be necessary.

Districts should consider the following items if applicable:

- Ensure that Active Directory passwords have been recently changed. Expired passwords may need LAN access to change.
- Ensure that personnel know their active directory credentials, as well as their credentials to other critical services (VPN, WyEd, email, etc).
- Test VPN access for employees that need it.
- Review employee internet accessibility and connectivity at home (via Speed Tests and other network diagnostics). Develop mitigation strategies or alternatives when necessary.
- Ensure that personnel have capable devices for work from home.
  - However, the use of personally-owned computers is discouraged. If necessary, ensure that these devices have proper security (antivirus, malware prevention, firewall configuration, etc).
- Ensure that all personnel understand that the use of personal devices for district business subjects those devices to public records requirements.
- Ensure personnel are able to log in to necessary resources remotely, and that credentials are working properly (web-based, locally hosted and other applications, network drives, shared resources, files, etc.).
- Provide employees with appropriate equipment (laptops, computers, etc) if necessary.
- Review internal and external communication plans with employees. Ensure that phones are forwarded if necessary.
- Ensure that IT Helpdesk personnel are accessible by staff. Contact information should be made readily available.
- Plan for an increased workload for IT staff during the transition to and from ‘Work from home.’
- Share a reminder of Security Best Practices with employees. For example, only using secure wireless connectivity and securing all PII, both electronic and physical (e.g., paper records).

- Ensure FERPA compliance standards are practiced.
- Provide a repository of shared resources or information (E.G. through Google Docs or Office 365) for staff to access. This could include an FAQ, voicemail instructions, employee directories, information from leadership, etc.
- Use standard collaboration tools (Zoom, Google Hangouts, Webex, Skype, etc.) and make them available to most staff. Additionally, consider employee training for these products.
- Ensure that designated staff can access all of our data collection systems remotely.
- Be aware of your surroundings when in a virtual meeting. Consider noise, who may hear the conversation, and what is in the background of your video.
- Ensure that IT personnel are apprised of operational plans and are intimately involved in decisions and execution.

For more information, contact Ken Reynolds at 307-777-8014 or **ken.reynolds@wyo.gov***.*