NEW YORK STATE REGIONAL INFORMATION CENTERS
DATA SECURITY PRACTICES FOR OFFSITE WORK

When working remotely, staff will face a number of data security and privacy challenges. Many will be similar to those faced while working in district, such as phishing emails and registering for online software. However, some additional challenges, such as virus protection and system updates, need to be considered as well.

WORK ENVIRONMENT

- Separate work area from non-work related activities.
- Take steps to keep sensitive information private from others.
- Shred any documents containing sensitive information.
- Connect to in-district resources only through authorized VPNs.
- Password protect remote office Wi-Fi networks.
- Use only approved software and tools to perform work functions.
- Follow established district policies and procedures.

DATA PROTECTION REMINDERS

E-MAIL PRACTICES

Exercise caution before clicking on a link in an e-mail or opening an attachment.

WORKSTATION PRACTICES

Ensure automatic updates are enabled on devices and antivirus software is installed.

Supported OS: Windows 8+, MacOS 10.14+

PASSWORD PRACTICES

Establish strong passwords. Do not write down passwords and leave in an easily accessible location.

DATA HANDLING PRACTICES

Use appropriate tools when handling data. Never send sensitive information through unencrypted email.

PRIVACY PRACTICES

Do not establish accounts for students to access online resources without consulting with administration.

PHISHING EMAILS

Phishing e-mails are one of the most common, and effective, methods cyber attackers will use to gain access to secure information.

1. **SENSITIVE DATA SHOULD ONLY BE SENT VIA SECURE EMAIL** or other secure transfer methods.
2. Exercise **CAUTION** before **CLICKING ON A LINK** in an e-mail or **OPENING AN ATTACHMENT**.
3. **REPORT SUSPICIOUS EMAILS** to your IT Department.
4. If you fall victim, **REPORT INCIDENTS** to your IT Department immediately.

REMAIN VIGILANT IN YOUR ENVIRONMENT