CYBERSECURITY GUIDELINES

FOR ALL STAFF

Keeping our computers and our data safe is a responsibility that we all share. You are our frontline defense against online threats. Here are some simple guidelines that all staff should follow:

1. Don't install software without permission. Speak to the system administrator if you need a piece of software to be installed on your computer.

2. Only save documents in the cloud or local network folder. Don't save documents directly to your computer, desktop, tablet, or phone.

3. Use a strong, unbreakable password made up of a mixture of uppercase and lowercase letters and numbers. Don't use the word "password" as your password! You can use this tool to see if your password is strong enough: https://www.vpnmentor.com/tools/passwordmeter/

4. Don't share a username and password with another member of staff. Make sure you have your own account.

5. Don't share your password with anyone, and don't put your password on a sticky note next to your desk – not even a virtual sticky note on your desktop!

6. If you get a suspicious-looking email from anyone (including an address that looks official, like Google) that asks you to share your password or any personal information, don't do it. Report the email to your manager and mark it as spam.

7. Don't open or download any attachments unless you know and trust the person who sent it.

8. If you're travelling for business, make sure your laptop and smartphone are with you at all times. Don't leave them unattended for any amount of time in a public place.

9. Attend all company training sessions on cybersecurity to get the latest guidelines.

10. Don't hesitate to ask if you have any questions, or see anything suspicious happening in your inbox, on the cloud, or on any company platform.

Together we can keep ourselves and each other safe online!