VAUGHN
NEXT CENTURY LEARNING CENTER

CYBERSECURITY AWARENESS GUIDE

Audience	All Employees, Faculty, Staff, and Contractors
Version	1.0
Effective Date	8/25/2026
Questions?	Contact the IT Help Desk via Fresh Service Ticket

Welcome

Every day, you help protect the students and families we serve, not just in the classroom, but every time you log in, open an email, or handle a student's record. Cybersecurity at Vaughn NCLC isn't just IT's job. It's everyone's job.

This guide covers what you need to know and do. It's short on purpose, the goal is that you actually read it and remember it. If you want the full technical policy detail, IT maintains the complete Cybersecurity Program Handbook and can answer any question you have.

VAUGHN
NEXT CENTURY LEARNING CENTER

Table of Contents

Welcome **2**
Table of Contents **3**
1. Your Top 5 Responsibilities **4**
2. Passwords and MFA, Made Simple **5**
Building a strong password 5
What is MFA, and why do I need it? 5
Keeping your password safe 5
3. Spotting Phishing and Scams **6**
Common red flags 6
What to do 6
4. Protecting Student and Employee Information **7**
Everyday do's and don'ts 7
5. Using Vaughn NCLC Devices and Accounts Safely **8**
6. Secured Technology Use **9**
7. If Something Goes Wrong: How to Report It **10**
8. Quick-Reference Cheat Sheet **11**
9. Your Annual Training **12**

1. Your Top 5 Responsibilities

1. **Protect your password.** Never share it, never write it down where others can see it, and use multi-factor authentication (MFA) whenever it's turned on for a system you use.
2. **Stop and think before you click.** Most cyberattacks start with one email or text message.
3. **Handle student and staff information carefully.** Only access what you need for your job, and only share it with people who are authorized to see it.
4. **Use only approved technology.** If you want to use a new app or online tool for Vaughn NCLC work, check with IT first.
5. **Report anything that feels off right away.** You will never get in trouble for reporting a mistake or a suspicious message. You may prevent a much bigger problem.

2. Passwords and MFA, Made Simple

Building a strong password

- At least 12 characters, longer is stronger. Think of a short phrase rather than a single word.
- Mix it up: include upper and lower case letters, numbers, and a symbol.
- Don't use your name, your username, Vaughn NCLC or the school mascot, or an easy pattern like "12345" or "aaaa."
- Never reuse your Vaughn NCLC password for a personal account, or a personal password for Vaughn NCLC systems.

What is MFA, and why do I need it?

Multi-factor authentication (MFA) means proving it's really you with something beyond just a password, usually a quick approval tap on an app on your phone. It's one of the single most effective ways to stop an attacker who has stolen or guessed your password. If a system asks you to set up MFA, please do it promptly.

> *Getting an MFA approval request you didn't ask for? Don't tap "Approve." Deny it and report it to IT immediately. It likely means someone has your password.*

Keeping your password safe

- Never share your password with a coworker, supervisor, IT staff member, or anyone else, legitimate IT staff will never ask for it.
- Consider using an approved password manager to generate and store strong, unique passwords.
- If you think your password may have been exposed, change it immediately and let IT know.

3. Spotting Phishing and Scams

Phishing is a fake email, text, or phone call designed to trick you into clicking a bad link, opening an infected attachment, or giving up information like your password or a wire-transfer approval. It's the number one way schools get hacked.

Common red flags

- Urgent or threatening language ("your account will be closed today").
- A request to buy gift cards, wire money, or change payroll direct-deposit details, especially if it claims to be from an executive.
- An unexpected attachment or link, even if it looks like it's from someone you know.
- A sender address that's almost right, but not quite (an extra letter, wrong domain).
- A message that pressures you to bypass normal procedures "just this once."
- A QR code in an unexpected email or flyer asking you to scan and log in.

What to do

- Pause. Legitimate requests can wait a few minutes for you to verify them.
- Verify unusual requests, especially money or payroll changes, through a separate, known channel (call the person, don't reply to the email).
- Hover over links before clicking to see where they actually go.
- When in doubt, forward it to IT or use your organization's "report phishing" button before you click anything.

From time to time, IT runs simulated phishing tests to help everyone practice spotting these messages. These are learning exercises, not "gotcha" traps, the goal is to build a habit that protects you and your students.

4. Protecting Student and Employee Information

Vaughn NCLC handles sensitive information every day, student education records, health and support-services information, staff personnel and payroll data. Protecting this data is both a professional responsibility and, for student records, a legal one under FERPA.

Everyday do's and don'ts

- Do: only access student or employee records you need for your current job duties.
- Do: send sensitive files only through approved, secure Vaughn NCLC systems.
- Do: lock your screen (Windows key + L) any time you step away from your device.
- Don't: email sensitive student or staff data to a personal email account.
- Don't: leave printed records containing student or staff information visible or unattended.
- Don't: discuss confidential student or staff information in public areas or with people who don't need to know.
- Don't: upload Vaughn NCLC data to a personal cloud account or an app IT hasn't approved.

5. Using Vaughn NCLC Devices and Accounts Safely

- Vaughn NCLC-issued devices remain Vaughn NCLC property. Use them for authorized school purposes.
- Don't install software or browser extensions that IT hasn't approved.
- Don't disable antivirus, firewall, or other security tools installed on your device.
- Keep your device with you or secured. Report a lost or stolen device immediately, even if you're not sure it's truly lost.
- Return Vaughn NCLC equipment promptly when requested or when you leave Vaughn NCLC.
- Only use technology and cloud tools that have been approved by IT for school business. New apps and "free" tools can create real security and privacy risks even when they seem harmless.

6. Secured Technology Use

- Connect to Vaughn NCLC systems only through the approved secure method (VPN or other IT-approved access), not an open or unfamiliar Wi-Fi network without protection.
- Keep your home Wi-Fi password-protected and your router's software up to date.
- Avoid working on sensitive information over public Wi-Fi (coffee shops, airports) without VPN protection.
- Make sure only you can see your screen when working in a public or shared space.
- Use only devices that meet Vaughn NCLC's security requirements to access sensitive systems remotely.

7. If Something Goes Wrong: How to Report It

If you see something suspicious, click something you shouldn't have, lose a device, or think your account may be compromised, tell IT right away. Fast reporting is the single biggest factor in limiting damage.

Report immediately if you notice:

- A suspicious email, text, or phone call
- A lost, stolen, or possibly compromised device
- An MFA prompt you didn't request
- Unusual computer behavior (pop-ups, slowness, files you can't open, ransom messages)
- Accidentally sending sensitive information to the wrong person
- Anything else that just feels wrong

How to report

Contact the IT Help Desk as soon as you notice the issue. Include what happened, when, and what you've already done (for example, whether you clicked a link).

> *You will not be disciplined for reporting a mistake in good faith. Not reporting, and letting a small problem become a bigger one, is the outcome we're trying to avoid. When in doubt, report it.*

8. Quick-Reference Cheat Sheet

Situation	What To Do
You got a suspicious email	Don't click. Report it to IT.
You clicked a bad link or opened a bad attachment	Disconnect from Wi-Fi if possible and tell IT immediately. Don't wait.
You got an MFA prompt you didn't request	Deny it. Change your password. Tell IT.
You lost a Vaughn NCLC device	Report it to IT immediately, even if you think you'll find it.
You need to share student or staff data	Use only approved Vaughn NCLC systems, never personal email or personal cloud storage.
You want to use a new app or website for work	Ask IT before you start using it.
You're working from home or a public place	Use the approved secure connection method; keep your screen private.
You forgot your password	Use the official reset process. Never ask a coworker for theirs.

9. Your Annual Training

All employees complete cybersecurity awareness training when they join Vaughn NCLC and at least once every year after that. Some roles (IT, HR/Finance, school leaders, and staff with access to sensitive student data) receive additional, role-specific training. You may also occasionally receive short reminders, simulated phishing exercises, or brief refreshers throughout the year; these are part of keeping the whole Vaughn NCLC community sharp.

Thank you for taking the time to read this guide and for helping keep Vaughn NCLC's students, families, and colleagues safe. If you ever have a question, about a suspicious email, a new tool you want to use, or anything else, the IT Help Desk is always the right place to ask.