includEd Learning

Independent Specialist Education Provider

CYBER SECURITY POLICY

Contents

➔ 1. Policy Elements

This Cyber Security Policy outlines guidelines and provisions for preserving the security of our data and technology infrastructure at IncludEd Learning.

This policy applies to all our staff, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements - Confidential data

Confidential data is secret and valuable. Common examples are:

- ➔ Financial information
- ➔ Staff Information
- ➔ Student information

All staff are obliged to protect this data. This policy provides guidance on how to avoid security breaches.

Protect personal and school devices

When using a device there is always a potential security risk to data. Staff should keep both their personal and school-issued devices secure. They can do this if they:

- Keep all devices password protected.
- Use antivirus software.
- Do not leave devices unattended.
- Install security updates of browsers when updates are available.
- Log into school accounts and systems through secure and private networks only.

We also advise staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

Staff should contact the Head of Centre if they have any questions.

➔ 2. Safer Practice

Keep emails safe

Emails often host scams and malicious software. To avoid virus infection or data theft:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.");
- Be suspicious of clickbait titles (e.g. offering prizes, advice.);
- Check email and names of people they received a message from to ensure they are legitimate;
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If a staff member isn't sure that an email they received is safe they should delete the email. If they are unsure, they should check with IT.

Manage passwords

Password leaks are dangerous. Passwords should be secure and remain secret. We advise staff to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays.)
- Remember passwords instead of writing them down. If staff need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- Change passwords every two months.

Transfer data securely

Transferring data introduces security risks. Staff must:

- Avoid transferring sensitive data (e.g. student information, staff records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request Staff to ask IT for help.
- Share confidential data over the school network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data have adequate security policies.
- Report privacy breaches and hacking attempts.
- Contact IT with any questions or concerns.

Additional measures

- Turn off screens and lock devices when leaving desks.
- Report stolen or damaged equipment as soon as possible.
- Change all account passwords at once when a device is stolen.
- Report a perceived threat or possible security weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software on school equipment.
- Avoid accessing suspicious websites.

We expect staff to comply with our Online Safety Policy.

We will:

- Install firewalls, anti-malware software and access authentication systems.
- Arrange for training to all staff.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow the policies provisions as other staff do.

In the event of an attack

- ➔ Do not click on any link that the ransomware provides for you.
- ➔ If something looks or feels suspicious raise it wit SLT.
- ➔ If you think a computer is infected - shut it down & switch everything off asap.

The Cyber Drill

Detect - Finding the issue - School/SLT
Isolate - Disconnect affected Device - School/SLT
Log issue with - School/SLT
Investigate - Smoothwall
Treat - Smoothwall
Monitor - School/SLT/Smoothwall
Report - School to report attack to Head of Centre/Smoothwall

Remote Staff

If working remotely, staff must follow this policy's instructions too. Since they will be accessing our school accounts and systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

Disciplinary Action

Staff who cause security breaches may face disciplinary action. This will be examined on a case-by-case basis.

DATE: AUTUMN 2023
NEXT REVIEW DATE: AUTUMN 2024
This document is reviewed annually to ensure compliance with current regulations.