The Challenge Academy Trust: Staff Working from Home IT Security Guidance Notes INTERIM

1. Introduction

As part of managing the coronavirus (COVID-19) situation, many organisations will be encouraging more of their staff to work from home. This presents increased cyber security challenges that need to be managed.

In addition, cyber criminals are preying on fears of the coronavirus and sending 'phishing' e-mails that try and trick users into clicking on a link to a malicious website (which could download malware onto your device or steal user passwords).

TCAT will continue to support learners where possible remotely through the use of Google Classroom, Moodle, Office 365 and the Remote Desktop/Gateway Systems as well other electronic resources.
Staff will be using collaboration tools, e-mail and other systems to communicate with other staff. It is important to remember that the same work-related cyber security rules apply at home this can sometimes be forgotten when working in a more familiar environment.

2. IT Equipment

Devices used for working outside an office environment are more vulnerable to theft and loss. Whether using your own device or equipment belonging to your school/college, ensure it is secure and not left unattended. If the device is portable and not being used, please keep it stored in a safe place.

If your work device is lost or stolen please report it as soon as possible to your **IT Support Team**. When outside of the normal working environment this can easily happen so early reporting will minimise the risk of a potential data breach.

When working from home it is more important than ever that you log out of any systems when you have finished using them. Online systems, including SIMS, REMS, G Suite applications, Office 365 applications and Remote Desktop/Gateway Systems etc, can be accessed with your usernames and passwords so it is crucial that you log out of all of these applications, especially on a shared home device. If you need to leave your home computer for a period of time unattended and you are logged into any online applications you must make sure the screen is locked in accordance to our GDPR policies.

3. Software Updates

Please keep your software and antivirus up to date on all of your home devices. Antivirus software should be installed on all home devices to protect from viruses / malware. Basic versions of antivirus are free and available for Windows, macOS, iOS and Android, including Sophos Home and TotalAV.

It is highly recommended that Antivirus software is installed on all portable equipment, including mobile phones and tablets. This software can identify and prevent malicious or potentially unwanted applications that may result in data theft, data loss and excessive network usage costs. If your device is lost or stolen, a remote lock or wipe will shield your personal information from prying eyes. Sophos Intercept X for mobile is free and available from Apple App Store and Google Play Store.

4. E-mail Phishing Scams

Reported cases of phishing and scam e-mails have increased over recent years - these are e-mails that attempt to persuade you to click on a link and provide personal details or financial account information.

Cyber criminals are preying on fears of the coronavirus and sending 'phishing' e-mails that try and trick users into clicking on a malicious link. Once clicked, the user is sent to a potentially corrupt website, which could download malware onto your computer or steal passwords.

Like many phishing scams, these e-mails are preying on real-world concerns to try and trick people into doing the wrong thing.

5. Spotting a Phishing E-mail

Until you're certain that the sender is genuine, you should not follow any links, or reply.
The next thing to do is try and identify whether the e-mail is a scam, or genuine.

Here are some tips on spotting phishing e-mails

- Many phishing e-mails have poor grammar, punctuation and spelling.
- Read the body of the e-mail carefully - is the design and overall quality what you'd expect from the organisation the e-mail is supposed to come from?
- If you've previously had e-mail contact from the company named in the suspicious e-mail, look over your prior communications and compare them to the new message. Do the writing styles, links, and domain names all match?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the e-mail contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet.
- Your bank, or any other official source, should never ask you to supply personal information from an e-mail.

6. Password Rules

Attackers will try the most common passwords or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

- Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.

- Report attacks as soon as possible to your **IT Support Team** - don't assume that someone else will do it. Even if you've done something (such as clicked on a suspicious link), always report what's happened.

- Use strong passwords as cyber-attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

- Use a separate password for your work account. If an online account gets compromised, you don’t want the attacker to also know your work password.

- Never reveal your password to anyone; your IT Support Team or other provider will be able to reset it if necessary.

7. Online Training

The training package below introduces why cyber security is important and how attacks happen, then covers four key areas of online safety. The training takes less than 30 minutes to complete and please note that it uses audio:

The four areas covered:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents ('if in doubt, call it out')

Stay safe online advice
https://www.ncsc.gov.uk/training/top-tips-for-staff-web/story_html5.html

8. Lesson Livestreaming

The following page highlights twenty safeguarding considerations for lesson livestreaming and explains how this should only be done when you are equipped to do so safely.

Twenty Safeguarding Considerations for Lesson Livestreaming

Just because schools are supporting students remotely and sending work home does NOT mean that you need to livestream lessons. This should only be done where you are equipped to do so safely. But if you are considering it, bear these things in mind:

1. Only use school-registered accounts, never personal ones
2. Don't use a system that your SLT has not approved
3. Will some students be excluded? Do they have internet, a device and a quiet place?
4. Do students and staff have a safe and appropriate place with no bedrooms or inappropriate objects/information visible?
5. Check the link in an incognito tab to make sure it isn't public for the whole world!
6. Has your admin audited the settings first (who can chat? who can start a stream? who can join?)
7. What about vulnerable students with SEND and CP needs?
8. Don't turn on streaming for students by mistake – joining a stream ≠ starting a stream
9. Never start without another member of staff in the 'room' and without other colleagues aware
10. Once per week may be enough to start with – don't overdo it and make mistakes.
11. Keep a log of everything - what, when, with whom and anything that went wrong
12. Do you want chat turned on for pupils? Can they chat when you aren't there?
13. Avoid one-to-ones unless pre-approved by SLT
14. Remind pupils and staff about the AUP agreements they signed* The rules are the same
15. Remind pupils and staff about the safeguarding policy and reporting process – does it work remotely?
16. Do you want to record it? Are students secretly recording it? You may not be able to tell.
17. How can students ask questions or get help?
18. What are the ground rules? When can students speak / how?
19. If you don't understand the system, if it won't be safe or reliable, if teaching won't be enhanced, DON'T DO IT.
20. Is your DPO happy? GDPR covered? Parental consent needed?

LGfL

DigiSafe

Keeping children safe

THE DIGISAFE TEAM WILL BE EXPLORING SAFE SETTINGS FOR THE MAIN PLATFORMS CHECK OUR SOCIAL PAGES

@LGfLDigiSafe

* Need templates?
See safepolicies.lgfl.net