IT Policy and Procedure

V1 22-23

I.T Policy

The purpose of this policy is to safeguard information assets, data and business knowledge. The Link Training Academy is heavily reliant on the use of computing and networking technology to effectively conduct day to day business and therefore it is essential we keep our data, devices and network as secure as possible, including achieving the Cyber Security Certificate and Enhanced Cyber Security Certificate by July 2021

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to relevant legislation. All employees are required to read and understand this policy and ensure they adhere to the company's rules when using IT Systems. All employees have a responsibility in managing the security of The Link Training Academy's data and information.

Working from Home

The Link Training Academy promotes flexible working as we recognise people have other commitments in their lives and we want to enable staff to enjoy a work life balance. This means that staff will be able to work from home if their role lends to this. Working from home increases the risk of security breaches and staff should make every effort to ensure they are keeping themselves and the company data safe and secure.
Staff should only work from a private residence with a secure Wi-Fi connection. They should not work from public coffee shops, libraries or on public transport where possible, if it is necessary then they should not use any guest wi-fi network and only access the internet through their mobile device's network or a private internet dongle. When working in public places, staff must use a privacy screen on their laptop.

Using a TLTA Laptop
If you are provided with a TLTA owned laptop devices, you should use this only for work purposes.

- Do not visit any websites that may possess a risk to the security of the device.
- Do not leave the device in an unattended vehicle.
- Ensure you are aware of the location of the device at all times
- Do not allow any other persons access to the laptop
- Only use an encrypted USB to save files and only if absolutely necessary.

Using your own device
You will not have access to The Link Academy's server or network from your own PC or mobile phone at any time. When on site at the academy, you will only have access to the guest Wi-fi log in.

At all times you must:

- Take all reasonable measures to prevent unauthorised access to your PC or mobile phone and keep them secure and password protected at all times. Use your device in an ethical manner at all times
- Only connect to TLTA's Guest WiFi connection
- Do not save any data relating to The Link Academy on your PC or phone unless necessary for remote delivery and then only save data onto an encrypted USB file

- Understand that any information or data relevant to your job role or TLTA which may be stored on a personal device remains the sole property of TLTA

Mobile Devices

We know that mobile devices such as mobile phones and tablets are convenient tools to use for work. If staff are using their personal mobile for work use they must follow the following rules;

- Use systems and equipment in a responsible manner and exercise good judgement
- Ensure devices and apps are updated as soon as possible
- Use strong passwords and set up fingerprint or face recognition where available.
- Back up any data using cloud based back-ups
- Enable encryptions (this is automatically enabled on iOS devices, android can enable it by going into Settings – Security – Encryption.
- Enable remote tracking so if devices are lost or stolen they can be tracked and erased.
- Do not "jail break" your device and/or install unapproved apps
- Do not connect to unsecure WiFi (i.e free WiFi in public places)
- Only connect to TLTA's Guest WiFi Connection
- Ensure devices are updated as soon as updates become available

The Link Training Academy reserve the right to wipe any device that is connected to TLTA's network and information systems in the event of a security concern. The Link Training Academy accept no liability for information lost from personal devices connected to TLTA's network and/or information systems.

Password Policy

When creating passwords all members of staff will follow these guidelines to ensure they keep themselves and the business as safe as possible from cyber threats and attacks;

- Always create passwords with at least 8 characters
- Consider adopting the "Three Random Words" policy
- Do not share your password with anyone else
- Do not write your password down, use a password manager if required
- Do not reuse a password you use for another account
- Do not use personal information in your passwords (such as birthdays, pets names etc.) as these are easier to guess by a hacker.
- Use two-factor authentication wherever possible as an extra line of defence.

Network:

To keep our data safe and secure on our network the server has a built in password policy. This policy sets requirements to ensure users are setting strong passwords; the policy ensure passwords have a minimum of 8 characters, are changed frequently and not reused. The policy does not have a maximum character limit to ensure users can chose an appropriate password. It is advised that users create a password using the "three random words" technique to create a suitably complex password that is memorable. The system is also set to lockout after 6 unsuccessful login attempts within 30 minutes.

The policy applies to both staff and student accounts that have access to the server. All Academy laptops and PC's will close down at midnight each evening, so always remember to save any work you require.

OneFile:
Staff members will also have an account for our e-portfolio software OneFile and will again need to create a suitably complex password for this. OneFile password policy ensures password are a minimum of 10 characters in length and are changed every 60 days. The OneFile system will also lock out any users after three failed login attempts; a Centre manager account will be required to unlock the account.

Emails:
Staff members will have a work email account that they should monitor daily. Emails can contain a lot of personal data and therefore need to be kept secure. The emails policy requires all users to set up two-factor authentication to provide an extra line of defence against hackers. A strong, unique password is still required even when two-factor authentication is enabled.

Other accounts
If staff members are creating accounts on other programmes/websites/apps for use at work they should follow the guidance above.

Reporting Lost or Stolen Devices

If one of your devices that is used for work is lost or stolen, you need to report it as soon as possible. The sooner this is reported the greater chance we have to recover the device or erase the data stored on the device before it is obtained by any unauthorised person.

All lost and stolen devices should be reports to Ben Lodge in the first instance.

Removable Media

All removable data must be kept on an encrypted USB following the password policy above. If you lose or misplace you data, you must inform Ben Lodge immediately to we can risk assess the damage and put measures in place to mitigate any risks as soon as possible.

CONTACT

You can contact Action Fraud, The National Fraud & Cyber Crime Reporting Centre, at any time if you think you've been attacked. Save their number in your phone: 0300 123 2040. You can also report via their website **https://www.actionfraud.police.uk** or use their live chat 24/7.