Cyber Essentials and IT Policy

This policy should be read in line with the Internet Policy, Data Protection policy, the Data Protection Act 1988 and GDPR.

Cyber Essentials

Cyber Essentials is a UK government information assurance scheme operated by the National Cyber Security Centre (NCSC) that encourages organisations to adopt good practice in information security.[1] It includes an assurance framework and a simple set of security controls to protect information from threats coming from the internet.

It was developed in collaboration with industry partners, including the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institution (BSI), and is endorsed by the UK Government.[2] It was launched in 2014 by the Department for Business, Innovation and Skills.

DHCT(A) ensures that all our data and ICT systems are compliant with Cyber Essentials and the protection of information and data at all times.

Information Security

Under no circumstances should you gain access or attempt to gain access to information stored electronically which is beyond the scope of your authorised access level.

Computer Software

- To avoid potential virus infection and consequent damage to the organisation, you must not load any software onto any computer without prior management approval. Approval will only be given after virus checking.
- Virus protection software is maintained and periodically updated.
- Under no circumstances must you load games or free issue software onto the organisation's equipment.
- If a specific application programme is necessary for your work, then it will be purchased by the organisation for your use.
- You must not make 'pirate' copies of organisation owned software for use by other persons either inside or outside the organisation. This not only breaks organisation rules, it is an illegal practice.
- Failure to comply with any procedure will give rise to disciplinary action taken against you, and this includes dismissal.

Electronic mail policy

- The use of DHCT computer system is provided for business purposes only. A small amount of personal use is permitted as long as it is not excessive and does not interfere with the normal business activity of the organisation.

- The company reserves the right to access employee's mailboxes to assist with technical problems or to investigate breach of this policy.

- Internet email is not a secure medium of communication. It can be intercepted and read. Do not use it to communicate anything you would not wish to be made public.

- Never expect any email messages you receive to be completely private.

- Emails might be seen during the course of maintenance work on the network particularly by authorised third parties.

- Do not forward email messages unless the originator of the message is aware the message may be forwarded.

- Do not sign onto email and leave your desk for long periods of time without logging off as it allows other employees direct access to your email.

- Always remember to disconnect from 'dial up' services once you have finished using Internet Explorer.

Staff are forbidden using electronic mail for:

Private business activities

- The receiving, sending or downloading abusive materials or offensive material to individuals or organisations.

- Sending chain letters

- Creating or forwarding email that contains abusive language. This includes racial or sexual discriminatory words and phrases.

This policy will be reviewed on an ongoing basis to maintain compliance

IT Issues Process

1. Where issues with the IT network is identified, the department relevant will be responsible for liaising with ITEC to raise a support ticket. Email support@itecgroup.co.uk and copy in e.west@dynamohealthcaretraining.co.uk

2. You can call ITEC on 01209 703 998 if immediate action is required.
3. The whole organisation IT Audit is maintained by Ellie Wiggin – support@dynamohealthcaretraninig.co.uk so she can keep the audit for the business up to date, but individual departments are responsible for keeping their own tracking of which member of staff and students have been allocated pieces of equipment.
4. It is the departments who are responsible for the IT equipment in their department and ensuring it is kept clean and working.
5. At the end of the AY all IT equipment is to be returned by students and staff, wiped of data, cleaned and set up for the new year.
6. Where a lock down occurs or a COVID outbreak and the department needs to self-isolate students can take equipment home, but they must sign a disclaimer to confirm that if they break the lap top they will be charged £300 and if they loose or break the charger they will pay £20.
7. In August before the Academy returns all computers need to be checked, set up and systems checked to ensure they are working properly ready for the students to commence. It is important that all 16 computers are turned on and linked to the system and printer at the same time to ensure the system doesn't have any issues. This will allow ITEC to resolve the issues prior to the students commencing for the year.

Academy Laptop set up process:

a. All laptops are wiped, Windows 10 Professional installed along with all updates
b. Microsoft Office, Adobe Reader and Google Chrome installed
c. Adobe Reader and Google Chrome set as default programs for PDF and Internet
d. Install printer drivers and make sure they all work with the WiFi and filtering correctly
e. Install ITEC TeamViewer and create a spreadsheet with all of their IDS
f. Before the Academy opens make sure all Laptops can connect to the network at the same time and print

To ensure that this policy is adhered to, the content of your email can, and will be monitored by Directors.