BIG CREATIVE EDUCATION APPRENTICESHIPS TRAINING ACADEMY

BIG CREATIVE ACADEMY
CLIFTON AVENUE
WALTHAMSTOW
LONDON, E17 6HL

TEL: 020 8498 3300
WWW.BIGCREATIVE.EDUCATION

IT SECURITY POLICY

Updated September 2019
Approved by the Principal

This policy links to and should be read in conjunction with the following policies:

- Guidance for Staff on Appropriate Conduct and Behaviour
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Parent Consent Form
- General Data Protection Regulation (GDPR) Policy

1. Introduction

1.1 Big Creative Academy operates across several sites and most staff members have access to many devices on which Academy business is conducted. The guidance below has been developed to ensure that Academy information is kept secure in accordance with the Academy's GDPR Policy (see also Appendix A on the key responsibilities for staff managing the technical environment at the Academy). Colleagues must take personal responsibility for their own devices and ensure the guidelines below are adhered to in order to ensure the security and integrity of data.

1.2 There is a particular focus on the use of social media at the Academy (see Appendix B). If you are at all unsure about any of the items in these guidelines please ask a member of the IT team to help you.

2. Email Security

2.1 Emails are generally not entirely secure and it cannot be predicted whether or not the correct recipient has received the email or whether it has been read by someone unintended. It is therefore generally unwise to send sensitive or confidential information via email.

2.2 Precautions should be taken to make sure the email has been addressed properly to the correct recipient.

- Do not leave emails logged in on any computer whether personal, work, internet café or any other place.
- Never give out your username and/or password to anyone and avoid writing down this information where others can obtain it.
- If emails are enabled on a mobile device, tablet or laptop users should ensure the device is well protected (pin lock etc.)

3. Phone Security

3.1 Mobile phones are prone to theft, hacking and other kinds of abuse. Correct precautions should be taken to avoid any security issues from arising.

3.2 Precautions should be taken along the following lines:

- Users must have a safe pin lock on their devices; pin locks should not contain guessable values such as '0000', '1234' etc.
- Smart phones have GPS integrated; this should be taken advantage of with apps such as 'Find my iPhone' (Apple) or 'Find my Phone' (Android) and many other similar products available in the app stores.
- Anti-virus apps should be used to prevent hacking / viruses entering smart phones.
- Devices should not be left in vehicles; should not be put down in public places and should remain with the owner at all times.
- Take note of the IMEI number in case of theft (this will allow the provider to block the phone from further use)
- Insurance should be considered and is highly recommended
- Bluetooth is no longer heavily used and should be turned off when inactive to avoid 'blue-jacking' (where individuals send anonymous messages containing viruses)
- Smart phones should be kept updated as much as possible (mobile phone firmware / operating system – updates are provided free from the manufacturer)

4. Personal Computer / Laptop / Tablet Security

4.1 Personal computers / laptops / tablets should not be considered 'safe' on the basis that the device is owned. Precautions should still be taken to ensure the safety of the device and user information.

4.2 Precautions should be taken along the following lines:

- Login username and password must always be enabled (no automatic login to a certain account).
- Passwords should not be left blank or be easy to predict such as "password", "bca"
- Apple devices are equipped with 'Find my iPhone' which can be used for all Apple devices (iMacs, MacBook Pros etc.) this should be enabled to trace lost / stolen Items and potentially catch thieves.
- Anti-virus software should always be installed and active to avoid hacking and / or viruses
- Programs such as iCam should be installed for monitoring your device as it uses inbuilt cameras or external webcams to monitor activity and notify owner (the camera feed can be accessed remotely using other devices)
- Ensure operating systems and all programmes are updated regularly in order to avoid being attacked
- Devices should not be left in vehicles; should not be put down in public places and should remain with the owner at all times.

5. Removable Storage Devices

5.1 Please do not use remote storage devices such as memory sticks or removable hard drives for sensitive data unless they are password protected.

5.2 If colleagues are frequently working at home they should set up a VPN to access the Academy's shared drive. Please ask the IT team for details.

5.3 In no circumstances should you email files to a personal address which contain sensitive data or save individual files on a personal device.

6. Use of photos/videos

6.1 The use of photos and videos featuring learners for internal use is agreed with parents and learners in the Parent Consent Form.

6.2 The use of photos and videos featuring learners for third party use is at the discretion of the Principal and learners' consent will be sought on an individual basis.

7. Web Filtering Systems

7.1 Big Creative Academy currently use Lightspeed Rocket as their web filtering application. This enables the Academy to restrict what websites a user can and cannot access over the internet.

7.2 The web filtering system contains keyword and content filters which will filter out websites that contain specific keywords or predefined content (such as pornography, for example). When a user types in a search query, the software determines, via the use of keywords or through access to previously databased information, what is contained on the site.

7.3 At the end of each month a monthly report is run on web filtering and passed to SMT. The monthly report will show the following:

- Users (staff & Students) who have been blocked
- Sites that have been blocked
- Users (staff or Students) who tried to access these suites or used works that have been blocked.

7.4 If a staff member would like a certain site unblocked for the duration of their lesson, then they should raise a Helpdesk call for the site to be unblocked for the day. The site will then be blocked again once lesson is over.

8. Securing the network from external threats

8.1 Remote Access: Big Creative Academy only use Cisco VPN; this is accessible by members of staff whom have been signed off by their line manager. Staff granted access have a time frame of two weeks before re-applying.

8.2 Security Levels: No user has the capability to install any software and would require admin access for ALL installations.

8.3 Server Access: All servers are not accessible offsite. They can only be accessed within the network.

8.4 All servers use Sophos Endpoint to eliminate any Virus threats.

8.5 Data port: At the Academy, any unused data ports are unpatched and therefore cannot be used to gain internet/network access.

8.6 Routine Patching: All computers onsite are updated on a regular basis; this includes software & OS. This stops any potential hackers that may target OS vulnerabilities.

8.7 Data: Faulty hard drives are always wiped before being collected by a HM Government approved data destruction company.

8.8 Users who leave Big Creative Academy, are immediately blocked from all Academy accounts and therefore have no access.