BIG CREATIVE EDUCATION APPRENTICESHIPS TRAINING ACADEMY

BIG CREATIVE ACADEMY
CLIFTON AVENUE
WALTHAMSTOW
LONDON, E17 6HL

TEL: 020 8498 3300
WWW.BIGCREATIVE.EDUCATION

IT SECURITY & USAGE POLICY

Updated July 2022
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

Introduction

All Big Creative Academy's information technology (IT) facilities and information resources remain the property of Big Creative Academy and not of particular individuals, teams or departments.

By following this policy, we will help ensure that IT facilities are used:

- Legally
- Securely
- Effectively
- Without undermining Big Creative Academy

The policy relates to all IT facilities and services provided by Big Creative Academy. This policy applies to all staff including the governing body, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for or provide services on behalf of Big Creative Academy (collectively referred to as 'staff' in this policy) as well as students and parents/carers and any other users of our IT are expected to adhere to the policy. Colleagues must take personal responsibility for their own devices and ensure the guidelines are adhered to in order to ensure the security and integrity of data.

The guidance below has been developed to ensure that Academy information is kept secure in accordance with the Academy's GDPR Policy.

1. Disciplinary measures

1.1. Deliberate and serious breach of the policy statements in this section may lead to the Big Creative Academy taking disciplinary measures. Big Creative Academy accepts that IT, especially the internet and email system is a valuable business tool. However, mismanagement of this facility can have a negative impact upon staff / students productivity and the reputation of the organisation.

1.2. In addition, all of the organisation's phone, internet and email related resources are provided for business purposes. Therefore, the organisation maintains the right to monitor the volume of internet and network traffic, together with the email systems. The specific content of any transactions will not be monitored unless there is a suspicion of improper use.

2. General IT Security

2.1. As a user of Big Creative Academy's equipment and services, you are responsible for your activity.

2.2. If you leave your PC or workstation unattended for any reason, you should lock the screen to prevent unauthorised access. If you fail to do this, you will be responsible for any misuse of it while you are away. Logging off is especially important when anyone else may be in the room and have access to the screen in your absence.

2.3. Do not disclose your system passwords or other security details to other employees, students, volunteers or external users, and do not use anyone else's log-in; this compromises the security of Big Creative Academy. If someone else gets to know your password, ensure that you get an IT team member to help you change it.

2.4. Any USB drives or other storage devices used on Big Creative Academy's network should be secure and encrypted. Please see section 'removable media' for more information.

2.5. Do not attempt to gain unauthorised access to information or facilities. The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorised access to any computer (including workstations/laptops etc.) or to modify its contents. If you do not have access to information or resources you feel you need, contact your line manager.

2.6. No user has the capability to install any software and would require an admin access (IT team) for all installations across the network.

2.7. All servers are not accessible offsite and can only be accessed within the network region.

2.8. All servers use Sophos endpoint to eliminate any virus threats.

2.9. Any unused data point within the academy is immediately unpatched and therefore cannot gain internet/network access.

2.10. All computers onsite are routinely patched allowing it to be updated on a regular basis, this includes software.

2.11. All faulty or unused hardware are always wiped before being collected by an approved government data destruction company. The destruction company is required to produce a destruction certificate for all hard drives handed over to the company for disposal

2.12. Users who leave the Academy are immediately blocked from all academy accounts and therefore have no access. IT team will/should get a formal email of authorisation for blocking of accounts.

3. Email

3.1. Use of email by staff and students is encouraged where such use supports the goals and aims of Big Creative Academy.

3.2. Keep email signatures short and include your name, title, campus, phone, Big Creative Academy logo & website address.

3.3. Use email in preference to paper to reach people quickly (saving time on printing) and to help reduce paper use.

3.4. Sending confidential information to external locations without appropriate safeguards in place.

3.5. Check your inbox at regular intervals during the working day, keeping your inbox fairly empty so that it contains items requiring your action.

3.6. Keep electronic files of electronic correspondence, only retaining what you need. Do not print it off and keep paper files unless absolutely necessary.

3.7. When publishing or transmitting information externally be aware that you are representing Big Creative Academy and could be seen as speaking on Big Creative Academy's behalf. Make it clear when opinions are personal. If in doubt, consult your line manager.

3.7.1. Do not open an email unless you have a reasonably good expectation of what it contains, and do not download files unless they are from a trusted source. For example, do open ***presentation.ppt*** from a colleague you know but do not open ***clickme.zip*** sent from an address you have never heard of, however tempting. Check the domain name of the email address (@domain.com) in the From: section of an email to help you decide identity of the sender. Alert a member of the IT team if you are unsure; this is one of the most effective means of Big Creative Academy protecting against email virus attacks.

3.7.2. Do not leave emails logged in on any computer whether personal, work, internet café or any other place.

3.7.3. Never give out your username and/or password to anyone and avoid writing down this information where others can obtain it.

3.7.4. If emails are enabled on a mobile device, tablet or laptop users should ensure the device is well protected (secure pin lock, fingerprint etc.) and ensure the device has a short power sleep, screen saver or lock time.

3.8. Improper behaviour

3.8.1. Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, discriminatory, offensive or abusive, sexist, racist, obscene, illegal or might be considered as bullying or harassment.

3.8.2. Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.

3.9. Confidentiality

3.9.1. Always exercise caution when committing confidential information to email since the confidentiality of such material cannot be guaranteed. Big Creative Academy reserves the right to monitor electronic communications in accordance with applicable laws and policies. The right to monitor communications includes messages sent or received by system users (staff and students) within and outside the system as well as deleted messages.

3.9.2. If you are sending, sensitive or confidential information via email then you must ensure that extra care is taken and the following protocols should be used:

3.9.2.1. Personal, sensitive and or confidential information should be contained in an attachment.

3.9.2.2. The attachment should be encrypted and or password protected.

3.9.2.3. Any password or key must be sent separately. Preferably using another form of communication e.g. phone call

3.9.2.4. Before sending the email, verify the recipient by double checking the email address. If appropriate, telephone the recipient to check and inform them that the email will be sent. If this is a first email communication with recipient, verify with test email first.

3.9.2.5. Do not refer to the information in the subject of the email. (I.e. **Subject: Password** - attachment: password.xlx).

4. Internet

4.1. Use of the Internet by staff and students is permitted and encouraged where such use supports the goals and objectives of the academy.

4.2. When using the Internet, staff and students must ensure that they:
4.2.1. Comply with current legislation.
4.2.2. Use the internet in an acceptable way.
4.2.3. Ensure not to create unnecessary business risk to the organisation by their misuse of the internet.

4.3. Improper behaviour

4.3.1. In particular, the following is deemed unacceptable use or behaviour by employees and volunteers (this list is non-exhaustive):
4.3.1.1. Visiting internet sites that contain obscene, hateful, pornographic or other illegal material;
4.3.1.2. Using the computer to perpetrate any form of fraud, or software, film or music piracy;
4.3.1.3. Using the internet to send offensive or harassing material to other users;
4.3.1.4. Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence;
4.3.1.5. Hacking into unauthorised areas;
4.3.1.6. Creating or transmitting defamatory material;
4.3.1.7. Recklessly introducing any form of computer virus into the academy network.

4.4. Confidentiality

4.4.1. Always exercise caution when using the internet, if you discover a website which you think should be blocked within the network please ensure you speak to a member of the IT team. Please refer to 'Web Filtering' for more information.

5. Removable Media

5.1. If storing or transferring personal, sensitive, confidential or classified information using Removable Media you must ensure you are following the protocols set:
5.1.1. Only use recommended removable media.
5.1.2. Encrypt and password protect.
5.1.3. Store all removable media securely.
5.1.4. Always consider if an alternative solution already exists.
5.2. Removable media must be disposed of securely by a member of the IT team.

6. Portable IT equipment

6.1. This section covers items such as laptops, mobile devices and removable data storage devices. Please refer to 'removable media' of this document when considering storing or transferring personal or sensitive data.
6.2. Use of any portable IT equipment must be authorised by IT.
6.3. All activities carried out on Big Creative Academy systems and hardware will be monitored in accordance with the general policy.
6.4. Staff must ensure that all data belonging to Big Creative Academy is stored on Big Creative Academy's network and not kept solely on a laptop. Any equipment where personal data is likely to be stored must be encrypted.
6.5. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of the car before starting your journey.
6.6. Ensure you synchronise all portable and mobile IT stored data, with the central organisation network server on a frequent basis.

6.7. Ensure portable and mobile IT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.
6.8. Installation on personal laptops of any applications or software packages purchased by the Academy must be authorised the IT manager, fully licensed and only then carried out by a IT team member.
6.9. In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight.
6.10. Portable IT equipment must be transported in a protective case if one is supplied.
6.11. Login username and password must always be enabled (no automatic login to a certain account). Do not put a sticker with login details, (username and password) on a laptop or any device.
6.12. Passwords should not be left blank or be easy to predict such as "password", "bca"
6.13. 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.
6.14. Anti-virus software should always be installed and active to avoid hacking and / or viruses
6.15. Ensure operating systems and all programmes are updated regularly in order to avoid being attacked.

7. Network files

7.1. Keep master copies of important data on Big Creative Academy's network server and Big Creative Academy's online storage facility (SharePoint & OneDrive) not solely on your portable disks. Not storing data on Big Creative Academy's network server and Big Creative Academy's online storage facility means it will not be backed up and is therefore at risk.
7.2. Ask for advice from a member of the IT team if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disk space very quickly and may bring the network to a standstill.
7.3. Be considerate about storing personal files on Big Creative Academy's network.
7.4. Do not copy files that are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disk space unnecessarily.

8. Use of Photos / Videos

8.1. The use of photos and videos featuring learners for internal use is agreed with parents and learners in the Parent Consent Form.
8.2. 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.

9. Communication

9.1. All communication between staff should be during the working day and via email, meetings, telephone or via text message on a work or school phone only.
9.2. Personal mobile phones should not be used for or during working hours or for communication regarding staff or pupils within the Academy.

10. Web & Network Filtering

10.1. Big Creative Academy currently use a web and network filtering application, enabling the academy to restrict what website a user can and cannot access over the internet.
10.2. The web filter system contains a keyword and content filter which will filter out website containing specific keywords or predefined content. (such as pornography, for example).
10.3. A monthly report is produced and passed on to SMT showing:
10.3.1. User's name.
10.3.2. Websites accessed in the past month.
10.3.3. Any blocked keywords that had been triggered.
10.4. The web and network filter is deployed across the entirety of network within the academy including laptops, tablets and workstations.
10.5. If a staff member would like a certain website unblocked for the duration of their lesson, they should raise a helpdesk ticket, the site will then be blocked after the duration requested.

11. Care of equipment

11.1. Do not rearrange the way in which equipment is plugged in (computers, power supplies, phones, network cabling etc.) without first contacting a member of the IT Team.