Farringdon Community Academy

ICT Policy

EXCELLENCE THROUGH ENDEAVOUR

UPDATED 10.05.18

Introduction

Farringdon Community Academy acknowledges that Information Technology is an important element of modern education. It opens opportunities for delivering the curriculum in innovative ways. However, the use of the many different mediums should be balanced with safety controls to protect the integrity of pupils and staff alike.

Purpose

- To protect the confidential data held on computer in the Academy from loss and corruption;
- To ensure the ICT mediums at our disposal are used ONLY for the purposes of delivering educational resources and not for personal gain;
- To protect children against malicious and unpleasant media and teach them how to use information technology safely;
- To adhere to the Data Protection guidance regarding how information is stored and used.

Scope

This Policy applies to all employees (including temporary, casual or agency staff and contractors, consultants and suppliers working for, or on behalf of, the Academy), students, third parties and any others who may use the Academy's ICT facilities.

The policy should be read in conjunction with the Academy Data Protection Policy.

Mobile Phone Policy

Students are discouraged from bringing mobile phones to the Academy but they are permitted. They are brought at the pupil's own risk and must remain switched off and kept concealed within the student's bag at all times.

If a student is seen with a mobile telephone their parent or guardian will be contacted and the device will be confiscated. It will be stored securely in the Academy safe and must be collected by the student's parent or guardian.

Staff must not use a mobile phone at a point where contact is with children. Mobile phone numbers must never be shared with students. The use of

personal mobile phones to take photographs of students or staff is strictly prohibited, and any member of staff or pupil found to be doing this, could face disciplinary procedures.

Cyber Bullying: (To be read alongside Anti-Bullying Policy)

The Academy takes the safety of its pupils very seriously and recognises that the use of information technology poses as many dangers as advantages. Cyberbullying can be defined as the use of Information and Communications Technology (ICT), particularly mobile phones and the internet, deliberately to upset someone else. It can be an extension of face to face bullying, with technology providing the bully with another route to harass their target

We will take a proactive stance on co-ordinating responsibility for cyberbullying and work with parents and children to identify instances where it could occur, and act where appropriate.

Promoting the positive use of technology:

ICT is increasingly recognized as an essential life skill, and embedding technology across the curriculum and in learning and teaching delivery provides opportunities and benefits for both learners and staff members.

We will work with children and staff to promote e-safety:

- Never give passwords to other people
- Change passwords regularly
- Do not upload images of children to websites under any circumstances
- Ensure pupil data held on computers is password protected
- Ensure firewalls and security centre updates are working effectively. When in doubt, advice can be sought from the ICT support team.

We will ensure that:

- Children only use the ICT resources in the Academy for the purposes intended i.e. solely for educational use.
- All interactive resources are from reputable educational suppliers (Education City etc) and have been installed with full child-friendly firewalls/safeguards.
- Children cannot access chat rooms or social networking sites when using Academy computers; access to such sites is automatically prohibited by the server.

Staff should reinforce the anti-cyberbullying code:

1. Always respect others
2. Think before you send
3. Treat your password like your toothbrush!
4. Block the bully!
5. Don't retaliate or reply
6. Save the evidence
7. Make sure you tell

ICT Internet Policy: Pupil and Staff Safety

The Academy has developed a set of guidelines for Internet use by both staff and pupils. These rules are made available to all staff and pupils, and kept under constant review.

All members of staff are responsible for explaining the rules and their implications. All members of staff need to be aware of possible misuses of on-line access and their responsibilities towards pupils.

By using the Academy's Internet access facilities, both pupils and staff agree to abide by the following rules to ensure safe and secure access:

Internet Access

- Internet access is only provided and supported for educational purposes – i.e. research, class-work or homework. Parental consent is required for students to access the internet and the use of the facility is a privilege, not a right and access requires responsibility.
- ICT users should only access the system with their own personal username and password, and must not pass their password onto others
- Staff and pupils should understand that their Internet access is constantly monitored and logged, as a precautionary measure.
- It is a disciplinary offence to download or access material on the Internet of an offensive or inappropriate nature.
- Anyone abusing or suspected of abusing his or her right to access the Internet may have his or her Internet access withdrawn.

The Following are not permitted

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using other's passwords

- Accessing and/or deleting other's folders work or files
- Intentionally wasting limited resources
- Downloading entertainment software or games or to play games against opponents on the internet
- Downloading images or videos unless there is a legitimate use for the Academy

Sanctions

- Violations of the above rules will result in a temporary or permanent ban on Internet use
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour
- When applicable, police or local authorities may be involved if particularly offensive material is found to have been downloaded.

Safety while "Online"

- Pupils should not pass on their personal details – name, address, telephone number, etc. – to other Internet users (e.g. via chat rooms, e-mail, etc.) unless specifically asked to by a member of staff, for educational reasons.
- Pupils must immediately report any unpleasant materials or e-mail sent to them to a member of staff, who will inform the appropriate Network Manager.

Downloading of Files

- Security controls prevent staff and students from downloading program files on Academy's PCs. It is an offence for a member of staff or a student to circumvent or attempt to circumvent these controls. Where a member of staff needs to download a program file they must ask a member of the ICT team to do so on their behalf.
- The Academy retains the right to use security software to monitor the use of all Academy PCs and Academy laptops, whether they are used at home or at the Academy.
- Students and staff should not use the internet to download music, audio or video files in the Academy unless they are relevant for teaching or coursework. This is due to the amount of excess network traffic which downloading this type of file generates. If any teacher needs to download a lot of such material they should liaise with the managed service.

ICT Security Policy

There are many aspects of ICT security that have been touched upon in the information included within this general policy.

The issue of ensuring data stored on computers is safeguarded is important and at the Academy, the following protocols have been introduced to ensure all information is stored in a safe environment and all equipment is appropriately accounted for:

- Pupil data compiled by staff is held confidentially and is password protected.
- Memory sticks and other external hardware storage devices are not permitted to be used under any circumstances.
- Photographs or personal data of children / staff must not be taken off site on portable media, or laptops.
- Student's work is saved on the curriculum server and can only be accessed remotely for the purposes of checking any software problems etc.
- When away from your desk for any period of time, you must lock your laptop or workstation and secure your room.
- Firewalls and Security controls are in place for both the curriculum and administrative servers.
- Data on the server is 'backed-up' regularly to ensure data can be retrieved in the event of accidental loss.
- Data is protected as far as possible against virus infection/malicious content with the use of effective security detection, which is regularly updated.
- Passwords should never be shared, they should be strong passwords (contain letters, numbers and symbols) and be changed regularly.

Laptop Policy (to be followed in conjunction with the ICT Security Policy above)

- All staff who have been allocated a laptop by the Headteacher must sign and agree to the Academy's laptop loan agreement.
- The laptop remains the property of the Academy.
- The laptop is allocated to a named member of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Academy Staff should use the laptop.
- On the teacher leaving the Academy's employment, the laptop is returned to the Academy. Staff on extended leave of 4 weeks and over should return their laptops to the Academy (other than by prior agreement with the head teacher).

- When in the Academy and not being used, the laptop must be securely stored in a locked office or drawer. It must not be left unattended at any time.
- Laptops must not be left in an unattended vehicle under any circumstances.
- Staff must not load their own software onto the laptop as this endangers the integrity of the Academy network.
- The use of memory sticks or any other external storage device is not permitted.
- It will be the responsibility of the member of staff to ensure virus protection software that has been installed on the laptop is kept up to date.
- Staff should not attempt to alter the computer settings other than to personalise their desktop working area.
- Students must never use the laptop.
- If any fault occurs with the laptop, it should be referred immediately to a member of the ICT team.
- When being transported, a sturdy fit for purpose laptop carrying case supplied must be used at all times.
- If not covered by standard household insurance the laptop should be kept within the Academy and locked up overnight.
- Personal data should never be stored on a laptop hard drive and taken off site. Access to data off site must be through Office 365, files should not be downloaded any editing should be online.
- When using a laptop off site you should never join an unknown WIFI network.
- Passwords must always be entered they should not be remembered.