Bailey Street AP Academy

ICT Security and E-Safety

This policy is available on our school website and is available on request from the school office. We also inform parents and carers about this policy when their children join our school and through our school newsletter.

The policy is provided to all staff (including temporary staff and volunteers) at induction alongside our Staff Code of Conduct. In addition, all staff are provided with Part One of the statutory guidance 'Keeping Children Safe in Education', DfE (2018)

This policy will be reviewed in full by the Governing Body on an annual basis. This policy was last reviewed and agreed by the Governing Body on [November 2020]. It is due for review on [April 2024].

Author: Mr S Cooksey Deputy Headteacher

Headteacher: Miss Lockett

Chair of the Local Advisory Board (LAB): Mr T Tweats

Publication date: 4/4/2022 Renewal Date: 4/4/2024

Amendments:
Section 7 of Acceptable User Policy (AUP) for Staff – Amended to include 6 monthly password changes, which must be 10 characters long. Multifactor authentication on selected school account for added security.

Bailey Street AP Academy - ICT Security and E-safety

Acceptable User Policy (AUP) for Staff

1.	Ensure you know who is in charge of the ICT system you use, i.e. their roles and responsibilities
2.	You must be aware that any infringement of current legislation relating to the use of ICT systems :- Data Protection Acts 1984 & 1998 Computer Misuse Act 1990 Copyright, Designs and Patents Act 1988 The Telecommunications Act 1984 may result in disciplinary, civil and/or criminal action.
3.	ICT resources are valuable and the confidentiality, integrity, availability and accurate processing of data are of considerable importance to the school and as such all users have a personal responsibility for ICT security. **Consequently, you must ensure that you follow all of the Academy's guidance, undertake appropriate training and complete relevant documentation in the use of your ICT system and in the storage and use of personal data (both e-data and hard data.)**
4.	Follow the rules in this AUP in relation to the use of private equipment and software and the personal use of the school's ICT system. All hardware and software used on the Academy's system is monitored for misuse by ENTRUST Monitoring Software. All software must be used strictly in accordance with the terms of its licence and may only be copied if specifically approved by the Office Manager and the ICT Technician. Staff are permitted reasonable personal use in their non-contact time providing such use is in accordance with the Academy's staff AUP. Staff must ensure all portable equipment provided for their use (and the data they contain) is stored securely both at work and at home. Staff must not use work laptops for storage of personal information, files etc including personal images (eg of your children) for use as screen savers. Staff must ensure that any personal mobile technology used at work sticks to the rules of this AUP.
5.	Ensure that wherever possible your display screen cannot be viewed by persons not authorised to see the information. Ensure that equipment is sited so as to avoid environmental risks, e.g. dust, heat. Do not leave your computer logged on, i.e. where data can be directly accessed without password control, when not in attendance. These same rules apply to official equipment used at home.
6.	You must not exceed any access rights to systems or limitations on the use of data granted to you by the Headteacher/Office Manager and ICT Technician.

7.	You are advised to change your passwords every 6 months. In some cases, these will be enforced by the system in use. You MUST NOT use the same password for your network and SIMs logon. You should not re-use the same password and make sure it is a minimum of 10 alpha/numeric characters, ideally a mix of upper and lower case text based on a “made up” word, but not obvious or guessable, e.g. surname; date of birth. Do not divulge your password to any person, or use another person's password, unless specifically authorised to do so by the Office Manager. Do not write your password down. In some cases where passwords are not enough, it is deemed necessary to use multifactor authentication for additional security.
8.	The ICT Technician will advise you on what “back ups” you need to make of the data and programs you use and the regularity and security of those backups.
9.	Any suspected or actual computer virus infection must be reported immediately to the Office Manager and ICT Technician.
10.	Due regard must be given to the sensitivity of the respective information in disposing of ICT printout and electronic data – follow the staff guidance on Information Security
11.	Users must exercise extreme vigilance towards any suspicious event relating to ICT use and immediately report any suspected or actual breach of ICT security to the senior leadership team or, in exceptional cases, the Headteacher, Chair of the LAB or Internal Audit.

12.	Staff must also be mindful of the dangers posed by the inappropriate use of social networking sites and are advised
	• Not to allow any current students
	  ○ to be friends/access to their private social networking addresses
	  ○ to have access to private phone numbers or e-mail addresses
	• Not to post any information related to their professional activities on social media
	
	Does your social networking/media compromise your professional identity and position within the school

13	Staff must also be mindful of the danger of **defamation** particularly with the expanding use of the internet. This includes being both a victim and perpetrator (not likely if you follow above advice) If you do believe you are a victim of defamation as a result of your professional duties, you must report it to the relevant senior teacher.
14	All activity carried out on a works/Academy’s machine is being monitored continuously. Any use/activity, which is found to include inappropriate, suggestive, confidential or illegal material that has been sent, received or created on this machine is a violation of the academy’s Acceptable Use Policy (AUP). Any user found to be in violation of the Academy’s AUP may be subject to disciplinary action.

Users of these facilities must complete the declaration attached to this AUP

Bailey Street AP Academy - ICT Security and E-safety

Acceptable User Policy (AUP) for Staff - Good Practice and Advice

E – Mail

***You should**:*

- check your E-mail inbox for new messages regularly
- use the recommended disclaimer as part of your signature when transferring classified data
- create your own contact groups rather than sending unnecessary mails – ask for help to do this
- treat E-mail as you would a letter, remember they can be forwarded / copied to others/deleted
- file mail when you have dealt with it and delete any items that you do not need to keep
- do a regular "spring clean" of all your e-mail folders
- ensure all classified personal data is only transferred as indicated by the school's guidance

***You should not**:*

- create wide-distribution E-mails (for example, to addressees throughout the school) unless this form of communication is vital
- print out messages you receive unless you need a hard copy
- send an E-mail that the person who receives it may think is a waste of resources
- Give out private home/personal e – mail addresses to students or parents

Folders and Documents held on School Network

***You should**:*

- Only keep regularly accessed files in your personal storage area
- Store archive files and delete folders/documents you will no longer use – do a regular "spring clean"
- There are many ways to store files eg external hard drives, cloud – ask for advice
- Ensure any classified personal data is held under the school guidance

You should not

- Copy folders/docs from a shared area into your personal area
- Add multiple files that eat up storage space (eg high resolution photos and videos)

Staff E-Safety

If you are the victim of any e – based bullying, receive any inappropriate material, believe you are a victim of defamation or have any other concerns you can contact a member of the senior leadership team.

The Academy will exercise its right to monitor the use of the Academy's computer systems. This will include access to websites, the interception of e-mail and the deletion of inappropriate material where it believes unauthorised use of the Academy's computer system is or may be taking place, or the system is or may be being used for a criminal purpose or for storing unauthorised or unlawful text, images or sound.

Bailey Street AP Academy - ICT Security and e-safety

Staff Declaration

You must read, understand and sign this form if you use our ICT facilities and services. We will keep the completed form in your personal file.

Declaration

I confirm that, as an authorised user of the Academy's ICT facilities, E-mail and Internet services, I have read, understood and accepted all of the Rules for ICT users in the attached **Acceptable User Policy for Staff (AUP**)

I confirm that I understand and will follow the Academy's guidance on the storage, use and transfer of classified personal data.

Name:

Job title:

Signature: **Date:**

This declaration should be returned to the Office Manager for safe storage

Bailey Street AP Academy

ICT Security and E- Safety Policy

Signed	Date

Chair of the local Advisory Board (LAB)

Signed	Date
Scott Cooksey	4/4/22

Deputy Headheadteacher