Policy A4 – ICT Acceptable Use

University of Brighton Academies Trust

1. Introduction

1.1 The Trust embraces any new and emerging technologies where educational benefits are seen to be available. There are many new digital resources being made available each and every day.

1.2 This policy is part of the Academies Trust Development Plan, and forms part of the wider policy framework in place in each Trust.

"The Internet and related technologies are powerful tools, which open up new prospects for communication and collaboration. Education is embracing these new technologies as they bring with them fresh opportunities for both teachers and learners. To use these technologies effectively requires an awareness of the benefits and risks, the development of new skills, and an understanding of their appropriate and effective use both in and outside of the classroom." DfES, eStrategy 2005

2. Scope

2.1 This document has been written in order to produce clear guidelines for everyone in the Trust community, including but not limited to staff (any-term), volunteers, agency staff, visitors, students and any other users of Information Communication Technology (ICT) at the Academies Trust. Hereinafter referred to as "Users".

2.2 This policy applies to all sites in the Trust however, where applicable, the individual sites may append additional guidelines to this policy based on a specific individual need or requirement. Therefore this would become non-exhaustive policy and we recommend that you check with your establishment directly to obtain the complete policy set applicable to you.

3. Purpose

3.1 The main purpose of this document is as follows:

- To safeguard and protect the children and users within the academy and Trust community,
- To safely embrace any new and emerging technologies if deemed to be of benefit to pedagogical practices within the Trust including but not limited to teaching and learning.
- To assist users working with children in the safe and responsible use of ICT and web-based services,
- To ensure that all members of the Trust and academy communities are aware of their professional and legal obligations in regards to ICT responsibilities and expectations while working for the Academies Trust.

4. General Guidelines for all Parties

4.1 Staff use of personal devices and mobile phones

4.1.1 Members of staff are not permitted to use their own personal phones, tablets, laptops, personal computers or similar devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Any pre-existing relationships which could compromise this will be discussed with managers/Principals.

4.1.2 Staff will not use personal devices such as mobile phones, tablets or cameras to take photos or videos of children and will only use work-provided equipment for this purpose if they have had permission to do so.

4.1.3 Staff will not use any personal devices directly with children and will only use work-provided equipment during lessons/educational activities.

4.1.4 Early Years staff will not use any personal phones and devices in classrooms or settings at any time

4.1.5 Members of staff will ensure that any use of personal phones and devices will always take place in accordance with the law as well as relevant Trust policy and procedures particularly Data Protection and Safeguarding in Education and Child Protection.

4.1.6 Staff personal mobile phones and devices will be switched off/switched to 'silent' mode during lesson times.

4.1.7 Bluetooth or other forms of communication should be "hidden" or switched off during lesson times.

4.1.8 Personal mobile phones or devices will not be used during teaching periods unless permission has been given by a member of the Leadership Team in emergency circumstances.

4.1.9 Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations.

4.1.10 If a member of staff breaches the Trust policy then disciplinary action will be taken.

4.1.11 If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted.

4.1.12 Any allegations against members of staff involving personal use of mobile phone or devices will be responded to following the Trust **Procedure for managing allegations of abuse made against staff members -** section 15 of Safeguarding in Education and Child Protection policy.

4.2 Visitors' use of personal devices and mobile phones

4.2.1 Use of mobile phones or personal devices by visitors and parents/carers to take photos or videos must take place in accordance with the Academy image use policy.

4.2.2 The Academy will ensure appropriate signage and information is displayed and provided to inform visitors of expectations of use.

4.2.3 Staff will be expected to challenge concerns when safe and appropriate and will always inform the Designated Safeguarding Lead of any breaches of use by visitors.

4.3 Security and Privacy

4.3.1 Users of Trust or academy ICT hardware, infrastructure or services must not disclose any password, login name given or security detail, to anyone, or allow anyone else to use their account. Re-use of "standard" passwords is also not permitted, passwords must be unique across services and accounts. Users must also ensure that passwords are sufficiently strong, in compliance with any and all security policies for the Trust.

4.3.2 No attempt to circumvent the security or protection of the Trust or academy network or any Trust or academy device is permitted.

4.3.3 Each Trust strongly discourages the use of removable media however if they are used to store any sensitive information we expect the use of strong encryption on all removable media (USB pen drives, CDs, portable drives) taken outside the locality of the academy or Trust office in any way e.g. sent off-site electronically or by post or courier.

4.4 Equipment / Hardware, Safe and Responsible use thereof

4.4.1 The consumption of food or drink is strictly prohibited whilst using Trust or academy hardware. It is hazardous to the equipment and to individuals.

4.4.2 Sensible, responsible and appropriate use of any Trust or academy hardware is expected at all times.

4.4.3 Laptops are portable, which allows the device to be moved from one location to another location, however using the device while moving from location to location is not permitted. Mobile devices such as tablets may be provided by the Trust or academy for mobile use where it is deemed to be required and applicable.

4.4.4 Under no circumstances should Trust or academy hardware be loaned for any term, to non-academy or Trust users. This includes but is not limited to user's friends, family or others.

4.4.5 Any device provided for your use, shall at all times remain the property of the Trust or academy. The Trust or academy reserves the right to require the return of its portable devices at any time.

4.5 Faults, Loss or Damage

4.5.1 Any faults should be reported promptly to the ICT Support Services team or local technician at the earliest opportunity. Loss of, or damage to the portable device should also be reported immediately to the ICT Support Services team, local technician or the Trust ICT Service Manager. In the case of theft, wilful damage or serious neglect you may personally be liable for the cost of the device/s in question.

4.6 Tampering and unapproved modification of devices

4.6.1 Under no circumstances should the operating system or installed applications on any Trust or academy provided devices be modified by the user in any way, this includes but is not limited to "Hacks", "Mods", "Jailbreaks", or any other actions that may interfere with the originally indented operation of the device.

5. Internet and E-Mail usage

5.1 Staff are not permitted to use "personal" e-mail accounts for any work-related purpose. Personal e-mail access is permitted, however this must be for personal use only. All official communications should be carried out using the official academy or Trust e-mail provided.

5.2 Use of e-mail and communication by e-mail should be treated with the same degree and care you would take if you were to write a letter to the person that you are contacting by email. It cannot be regarded as purely private, only to be seen by the receiver. E-mail can be stored, forwarded and distributed to large numbers of people at the touch of a button. It is easy to forget that it is a permanent form of written communication and that material can be recovered even if seen to be deleted from the computer.

5.3 When using e-mail, users should:

- Be aware that e-mail is not a secure form of communication and therefore no personal information should be sent,
- Not forward e-mail messages onto others unless the sender's permission is first obtained. Especially in cases where the communication is outside of the organisation.
- Must not open e-mail attachments from unknown senders,
- Must not send e-mail messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive

5.4 The guidance in this policy will apply to any electronic communication, including but not limited to e-mail, web services, chat rooms, forums, bulletin and news group or peer to peer sharing etc.

5.5 Please remember that each academy email system is owned by the Trust and any mail arriving at this email system is the electronic property of the Trust. The email system may be monitored and interrogated by the ICT Support Services team.

5.6 Inappropriate material

5.6.1 Under no circumstances should users view, upload or download any material that is likely to be unsuitable for children or users at each academy or Trust. This applies to any material of violent, dangerous, racist, or inappropriate sexual content. If users are unsure about this, or any materials, users must ask their line managers or the ICT Service manager. If in doubt, do not use. The transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to personal prosecution by the police.

5.6.2 Any unsuitable or inappropriate materials found on an academy or Trust network or the Internet, by accident or otherwise, must be reported immediately to the ICT Support Team. Details must include the location and nature of the material including the Internet addresses (URLs) where applicable to allow removal or filtering to be applied, or for disciplinary action to be taken if appropriate.

6. Copyright and Licencing

6.1 Users accessing software or any services available through an academy must be in compliance with any licence agreement and/or contract terms and conditions relating to their use and must not alter or remove copyright statements. Some items are licensed for educational or restricted use only.

6.2 Do not download, use or upload any material that is subject to third-party copyright. Always seek permission from the owner before using any material from the Internet. If in doubt, or you cannot obtain permission, do not use the material.

7. Guidelines for Staff - remote access to academy or Trust systems (VPN)

7.1 Where approved, remote access enables you to work on files and potentially have access to SIMS / The MIS and other school systems and data from off-site. This increases the risk of other people gaining access to important and confidential information and means that staff need to be particularly vigilant when leaving their device unattended if using Remote Access. The Information Commissioner's Office (ICO) has judged both schools and individuals very harshly when lax procedures and practice have resulted in data protection breaches.

7.2 VPN/Remote access is provided to any user on a case-by-case basis. Requests for access should be made by a user's line manager; requests may be refused and previously approved access may be revoked without justification.

7.3 VPN usage must adhere to all existing Trust policies and comply with all public legal frameworks including, but not limited to, Data Protection legislation.

7.4 All users hereby agree that VPN usage data (Connection times, IP address', file access etc) is recorded and subject to audit.

7.5 VPN usage potentially leverages a user's personal / home internet connection. Therefore connection quality may vary and additional service charges may apply, dependent on a user's service plan subscription.

7.6 VPN software and connections should only be used on Trust or academy owned devices. Connections from personal devices is forbidden and no attempt to setup the software and connection on personal devices should be made.

7.7 With the VPN connection active, all communications traffic will be directed through the Trust or academy network and will be subject to controls, policies and network/firewall restrictions.

8. Use of cloud-based storage and services

8.1 The Trust does not endorse the use of one particular cloud-based solution over any other. However any chosen system must have completed the Department for Education' self-certification checklist (details of which can be found here: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act). The Trust do insist that any system used is done so in a managed, informed and legal way. Including adherence to the following guidelines.

8.2 Managed use – At all times the individual data controlling entity retains full responsibility for how the data they control is used and accessed. Therefore a method of securing and managing access to the data, including audit functions and potential revocation of any user's access to the data, is essential and must be ensured by the controlling entity.

8.3 The transfer of any data to any cloud service does not transfer liability or responsibility away from the controlling entity. Any and all legal frameworks are still applicable in regards to data protection and use of the data.

8.4 The Trust strongly recommend that no sensitive or personal data be transferred, for any term, to any cloud service. Usage should be limited to collaborative working and strategic data rather than any sensitive or personal information.

9. Breaches of policy

9.1 Any violation of the standards, procedures or guidelines set out in this policy may be treated as a formal Trust disciplinary matter, which could result in dismissal, legal prosecution or both.

10. Legal frameworks

10.1 It is the user's responsibility to ensure they are compliant and work within all UK and E.U. applicable legislation in regards to the safe and legal use of ICT at the academy or Trust, this includes but is not limited to the following:

- The Sexual Offences Act 2003
- The Racial and Religious Hatred Act 2006
- The Computer Misuse Act 1990 (sections 1 – 3).
- The Police and Justice Act 2006
- Communications Act 2003
- Data Protection Act 1998
- Malicious Communications Act 1988
- Copyright, Design and Patents Act 1988
- Public Order Act 1986
- Protection of Children Act 1978
- Obscene Publications Act 1959 and 1964
- Protection from Harassment Act 1997.
- The Regulation of Investigatory Powers Act 2000 (RIP)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2002 (Keeping Children Safe in Education September 2016)
- Childcare Act 2006 (The Early Years Foundation Stage (Welfare Requirements) Regulations 2012

11. Definition of terms

"Confidential" or "sensitive" information includes, but is not limited to:

- Person-identifiable information, e.g. student and employee records protected by the Data Protection Act 1998,
- Information divulged with the expectation of confidentiality,

- Academy, Trust or County Council business or corporate records containing organisationally or publicly sensitive information,
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and politically sensitive information.

"Remote access" - Non-local access to any academy/Trust system/s or services,
"VPN" – Virtual private networking. Technical terminology for "remote access",
"Licence" - An agreement between two parties for use of a specific system or service,
"Upload" - The act of publishing any data on the internet or cloud service, in any way perceived public or private,
"Download" - The act of copying or removing data from the internet or cloud service
"Mobile use" - Use of any hardware while mobile in any way.

12. Policy status and review

Written by:	Governance Manager
Owner:	Director of ICT
Status:	approved
Approval date:	V1 = UoBAT – Board of Directors 10/12/15 V1 = HAT – Board of Directors 17/12/15 Minor amendments made to joint policy March 2016 V2 = UoBAT/HAT Board of Directors May 2017 Merger editorial changes 1 September 2017
Review Date:	As required or May 2019