Policy A4 – ICT Acceptable Use

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.

“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 device to share content directly with children

4.1.4 Staff should consider “muting” smart watches or other wearable technologies whilst in the classroom to avoid notifications/messages being shared with children.

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 and Child Protection.

4.1.6 Staff personal mobile phones and devices will be switched to ‘silent’ mode during lesson times.

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

4.1.8 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.

4.1.9 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 9 of each academy’s Safeguarding 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 of safe and appropriate ICT use 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. 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 Users must lock their desktop, laptop, or mobile device when away from it.

4.3.4 2 Factor authentication (2FA/MFA) is to be used by all Trust employees where computer access is required.

4.3.5 Users must keep their device up to date. Devices will automatically prompt when updates are available, but it is the user's responsibility to ensure that they follow the prompts and carry out the actions required to keep the device updated and safe.

4.3.6 ICT services strongly discourages the use of removable media to store and transport files. However, if it is used the device must be encrypted. This includes the use of USB pen drives, SD Cards CDs, DVDs, mobile phones and portable drives. Digital cameras tend not to support encryption so extra care should be taken to ensure that the content stored is reviewed and exported/ cleared regularly.

4.3.7 Staff may need to login to services such as office 365 email on a device that is shared with other users outside of our organisation. An example of this would be the use of a home pc or a public computer at a training event. In situations like this you should be mindful of tools that could be installed on the computer to capture sensitive information. PCs in hotel lobbies or public internet cafes are risky as criminals may have interfered with the device prior to your visit. Systems operated within training centres and other commercial establishments are usually much less likely to have been interfered with. If you have any suspicion on the safety of the PC/device, do not attempt to login to your account. Critically, even on trusted devices including your home pc, ensure that you sign out of your account before you leave the desk.

4.3.8 Any concerns regarding any aspect of security should be raised immediately by emailing safer.it@brightonacademiestrust.org.uk

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 phones and 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.

4.4.6 Staff may choose to add a label / sticker to a device to aid identification. Careful consideration must be given to ensure that any form of modification will not damage the device and that it is removed / cleaned before returning the equipment to back to ICT services.

4.5 Faults, Loss or Damage

4.5.1 Any faults, loss, or damage to items loaned to you including peripherals (chargers and headsets) should be reported promptly to ICT Support Services - ICTHelp@BrightonAcademiesTrust.org.uk

4.5.2 In the case of theft, wilful damage or 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 device 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 intended operation of the device.

5. Internet and communication system usage

5.1 Staff are not permitted to use "personal" e-mail accounts or communication platforms such as WhatsApp or Telegram for any work-related purpose. All work communications should be carried out using the official Trust provided services i.e. Microsoft 365 email and Teams.

5.2 Use of e-mail and Teams should be treated with the same degree and care that would be taken if writing a letter to the person that you are contacting. It cannot be regarded as purely private, only to be seen by the receiver. Electronic communications 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 Members of staff are encouraged to maintain an appropriate work life balance when using electronic communications, especially if this is taking place between staff, students/pupils and parents.

5.4 When using e-mail or Teams, users:

- Should be aware that by default e-mail is not a secure form of communication unless the encrypt function has been enabled before sending.
- Should not forward e-mail or instant 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 file attachments from unknown senders,
- Must not send messages in the heat of the moment and avoid writing anything that may be construed as defamatory, discriminatory, derogatory, rude or offensive

- Should be aware that in the event of a Subject Access Request, what you have written about them will likely be provided as part of the request.

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

5.6 All communication systems may be monitored by the ICT Service team.

5.7 Inappropriate material

5.7.1 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.

5.7.2 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.

5.8 Profile pictures

5.8.1 Online services such as Office 365, helpdesks, social media and other similar platforms allow users to upload a profile picture. Staff using these platforms in a professional capacity should only upload a professional/smart photo to aid other colleagues and students in identifying them; photos should be a head and shoulders picture with a neutral background. Avatars or photos of a social nature must not be used.

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 permission cannot be obtained, do not use the material.

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

7.1 Where approved, remote access enables users to access SIMS and other school systems whilst 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. 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 the need for the Trust to provide 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.

8. Use of cloud-based storage and services

8.1 The Trust fully endorses the use of Microsoft Office 365 and it is the expectation that this is the only cloud-based storage system in use for all Trust related documents and communication.

8.2 Staff should not use other platforms such as Google Drive, Google Suite or Dropbox to store or transfer work between devices / colleagues. It is accepted that some third-party companies will provide content on these services for you to download.

9. Live streaming of lessons

9.1 Staff participating in online streaming of lessons or using video conferencing to contact pupils/students will follow guidance issued “Using Office 365 for remote learning – Guidance for Staff” – Annex A

10. Breaches of policy

10.1 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.

11. Legal frameworks

11.1 It is the user’s responsibility to ensure they are compliant and work within all relevant 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 2018
- 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

12. 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 2018,
- 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.
“Live stream” - a somewhat broad term and, in some cases, can refer to a platform where the teacher and the children are all linked into a video call/conference and see one another. In other cases, it may refer to a live broadcast, where only the teacher, or whoever is providing the content, is visible and the children are viewing the content, without being seen themselves. In the latter example, although not linked into the broadcast with their images, the children may be able to interact through a live chat function.

12. Policy status and review

Written by:	Head of Governance and Admissions/Director of ICT
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
	V3 = 02-12-19 Finance and Resources Committee
	V4 = Chair FRC 23-09-2020
	V4a = minor amendment to operational guidance on attendance and staff presence in online lessons only
	V4b = minor amendment to operational guidance on use of pupil cameras

	V5 = Chair FRC 26-02-2021
	V6 = Chair FRC 06-07-2022

Summary of latest changes	V6 = updated to reflect use of 2FA and in line with current guidance
Review Date:	As required or September 2023

Annex A

Using Office 365 for remote learning

Guidance for Staff

1 Introduction

The University of Brighton Academies Trust provides Microsoft Office 365 access for staff and pupils across all Academies. This service offers exciting opportunities for remote learning that have not been previously possible.

With opportunities there are new risks that this guide will help you manage.

The office 365 suite offers the following services: -

Microsoft Teams – Channels and Files (Video/Audio/Text Chat/Resources)	Allows staff to set up controlled Teams (groups of pupils) and collaborate in a number of ways. This includes the use of text chat, video and/or voice as well as the sharing of resources (including Word, Excel and PowerPoint documents)
Microsoft Stream	Allows staff to pre-record lesson content and upload it to the Academy website or share direct links to pupils to watch.
Microsoft Teams – assignments (This currently only applies to secondary sites)	Allows staff to set work for students to complete it and send it back for marking and feedback. This also includes quizzes and an online gradebook.

This document focuses on Microsoft Teams and sets out guidance to ensure you and your pupils remain safe whilst using the video/audio and text chat elements of this technology.

First and foremost, it is important to think of your Class Team as a traditional classroom. Any files that you upload can be viewed by all of the students. Any posts that are shared in the feed can also be viewed by all students. Therefore, do not upload or share anything that you would not normally do so in your classroom. Also, please note that Office documents will be editable by all users when you upload them. If you want to upload material that is simply for reference either set the file to 'view only' or upload a PDF version instead.

In terms of live streamed lesson:

As a staff member you can do the following easily during a session: -

- Choose which pupils you allow to enter your Team.
- Remove a pupil from a Team.
- Mute one or all pupils so they cannot speak.
- Delete unwanted posts or files that have been created by pupils.

By default, we have restricted pupils: -

- Students have no access to control the meeting including muting anyone other than themselves.
- They can post or comment within a class/meeting, but they cannot delete or edit the post or comment.
- Students accounts can also post comments and replies to posts in the main feed unless you have set your post to not accept replies. As above students cannot edit or delete their posts but you as the Team Owner can. Any comments or replies that do not adhere to the Academy code of conduct should be treated in the same way as they would be in a normal classroom.
- They can upload work for assignments that you have set as the teacher. They can see their individual feedback and grades but will not see the class gradebook.

Full training videos can be found in ICT services on the Office 365 Intranet

2 Protocols to keep you and your pupils safe

- When students join a live call, they should be asked to disable their webcam and only enable it when requested by a member of staff.
- Staff can at any point raise a request with ICT service to permanently disable individual student webcam functionality if they feel the student has abused this feature.
- Two members of staff will be 'within the Team (in the same room at school, or if working remotely, in the video call) when conducting a live stream session with pupils.
- The second member of staff is there to provide a safeguard for both the pupils and the teacher, so does not need to be a curriculum specialist.
- The second member of staff could act additionally as technical/behaviour support, in terms of monitoring pupils' interactions and ensuring they are not using chat or other functions inappropriately.
- The second member of staff does not need to be present for the whole remote session but does need to gauge a view of safeguarding. We recommend they remain in the session for a minimum of 20 minutes.
- Sessions will be planned and scheduled for during school hours. If you need to run a session outside of normal school hours you will need to seek approval from a member of your academy leadership team.
- Parents will be contacted to advise that the session is taking place and they and the pupil should consent to abide to an acceptable use agreement covering issues such as not recording the session and being appropriately dressed etc.
- Only school contact numbers/emails will be used for communications and running the session i.e. staff should never issue their personal contact details.
- The only live streaming platforms approved is Microsoft Teams from the University of Brighton Academies Trust Office 365 tenant.
- Live streaming sessions should not be recorded.
- Live events should not occur with other members of your household present.
- Where inviting students as guests (via a link), ensure settings are set to 'admit from the lobby' therefore pupils cannot join without your knowledge. Note – this is set by default.
- Staff should be aware of open applications including website tabs if using the screenshare functionality.
- Staff will dress professionally and choose a neutral background for their video stream.
- 1:1 video call sessions to support interventions with pupils such as mental health support or counselling will only be provided where they have been risk assessed and approved by SLT.
- At the end of the class, a member of staff should end the meeting to ensure all pupils are removed from the call rather than hang-up.
- Staff behaviour and language will be entirely in line with the staff code of conduct.
- Staff should read the Using Office 365 for remote learning guidance for pupils, so you fully understand the expectations of them during a session.
- All other school policies/practices should be followed, notably the safeguarding and pupil protection policy so should there be any welfare concerns about the pupil these should be brought to the attention of the DSL without delay.
- In most circumstances' attendance will need to be recorded :-

Primary – Please continue to follow attendance coding guidance issued on 11.01.2021. There is a remote learning tracker available for each infant and primary academy. This spreadsheet will enable each academy to track and analyse engagement with remote learning. The tracker will support you to identify any missing children. Each tracker will calculate average hours of engagement for each year group and vulnerable cohorts. Links available on SharePoint. Please submit remote learning data centrally, as requested.

Secondary – Please continue to follow attendance coding guidance issued on 11.01.2021. Create a tracking system that enables you calculate the average number of hours engagement and to identify any missing children. The School Improvement and IT teams can support you with this. Face-to-face and live lessons, that run in sync with timetable lessons, can continue to be recorded on SIMS registers. Contact the Trust Attendance Manager/Interim Safeguarding and Welfare Lead for current attendance coding advice in secondary settings. Please submit remote learning data centrally, as requested.