BASINGSTOKE ALLIANCE SCITT

Acceptable Use Policy and Agreement

Policy Title		Acceptable Use Policy and Agreement		
Author / Reviewer		Data Protection Lead		
Trustee Committee		Delegated to the Headteacher		
Signed by Chris Toner (Interim Headteacher)				
Reviewed June 2021	**Approved**	June 2021	**Next Review**	June 2023

Introduction

This policy is designed to enable acceptable use for BASCITT trainees. This policy covers all individuals training within all routes, provider led core, school direct tuition, school direct salaried and apprenticeship. They are collectively referred to as "**trainees**" in this policy.

The Basingstoke Alliance SCITT (BASCITT) provides ICT resources which are available to trainees. To ensure the safety of trainees and pupils, it is important that all staff, including trainees, follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the BASCITT's ICT systems and infrastructure.

- Define and identify unacceptable use of the BASCITT's ICT systems and external systems.

- Educate users about their data security responsibilities.

- Describe why monitoring of the ICT systems may take place.

- Define and identify unacceptable use of social networking sites and school devices.

- Specify the consequences of non-compliance.

This policy applies to trainees and all users of the BASCITT's ICT systems and as such they are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by trainees, and monitoring by the BASCITT, of its electronic communications systems is likely to involve the processing of personal data. It is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff, including trainees, are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Data Protection Lead.

Provision of ICT Systems

All equipment that constitutes the BASCITT's ICT systems is the sole property of the BASCITT.

No personal equipment can be connected to or used with the BASCITT's ICT systems. Memory USB sticks must be encrypted and can only be used if they are provided by the BASCITT.

Users must not try to install any software on the ICT systems without permission from the BASCITT. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

BASCITT is responsible for purchasing and/or allocating ICT equipment to individuals. Individual ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Users are not permitted to make any physical alteration, either internally or externally, to the BASCITT's computer and network hardware.

Network access and security

All users of the ICT systems at the BASCITT must first be registered. Following registration, a Google Classroom user account will be created, consisting of a username, password and an e-mail address. All passwords must be complex to ensure data and network security and should include 8+ characters, at least one upper case letter, at least one number and one special character. All user account details are for the exclusive use of the individual to whom they are allocated. Trainees are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to the IT Manager and IT Provider for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the BASCITT Programme Director as soon as possible.

Users can only access areas of the BASCITT's Google Classroom to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the BASCITT ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the BASCITT ICT systems or cause difficulties for any other users.

Under no circumstances can a pupil be allowed to use a trainee's computer account.

BASCITT Email

Where email is provided, it is for academic and professional use, with no personal use being permitted. The BASCITT's email system can be accessed from both the SCITT ICT equipment, via the internet from any computer or phone via an app. Wherever possible, all BASCITT related communication must be via the BASCITT email address.

The sending of emails is subject to the following rules:

- Language must not include swear words or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the BASCITT or placement school does not have distribution rights is not permitted.
- The use of personal email addresses by trainees for any official BASCITT business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email or password protection.
- Emails must never contain pupil's full names either in the subject line and not in the main body of the text. Initials must be used wherever possible.
- Access to school /setting email systems will always take place in accordance with data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell the BASCITT Programme Director and Headteacher of their placement school if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Trainees will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations must be written carefully and checked before sending, in the same way as a letter written on BASCITT headed paper would be.
- BASCITT email addresses and other official contact details will not be used for setting up personal social media accounts.

- Where possible emails must not contain personal opinions about other individuals, e.g. other trainees, BASCITT/DHAS/placement school staff, pupils or parents. Descriptions of individuals must be kept to a professional and factual manner.

Internet Access

Internet access is provided for academic and professional use only.

Placement schools' internet connections are filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately following the placement schools' acceptable use policy.

Trainees must not therefore access from the placement school's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- Accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials.
- transmitting a false and/or defamatory statement about any person or organisation.
- sending, receiving, downloading, displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others.
- transmitting confidential information about the BASCITT, DHAS or placement school and any of its trainees, staff, pupils or associated third parties.
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the trainee, the BASCITT, DHAS or placement school).
- downloading or disseminating material in breach of copyright.
- engaging in online chat rooms, instant messaging, social networking sites and online gambling.
- forwarding electronic chain letters and other materials.
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action.

Where evidence of misuse is found the BASCITT may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital cameras

The BASCITT provides ICT equipment for the purposes of digital recording. Trainees must be aware of the following guidelines:

- Photos cannot be taken of pupils or staff.
- Photos must only be named with the pupil's or staff's initials. E.g., sample of pupil work.
- The use of personal digital cameras in placement schools is **not** permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos must be downloaded to the BASCITT Google Classroom as soon as possible.

File Storage

Trainees have their own personal area on Google Classroom. Any BASCITT programme related work must be stored on one of these network drives. **Personal files are not permitted on Google Classroom or local areas.** Trainees are responsible for ensuring they have rights for the storage of any file in their area, for example copyright music files. Any files stored on removable media must be stored in accordance with the information access and security policy, summarised as follows:

- If information/data must be transferred it must be saved on an encrypted, password protected, storage device.
- No BASCITT, DHAS or partnership school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act can be transferred off site.

Mobile Phones

Trainees are required to follow their placement school policy for the use of mobile phones.

Social networking

The key requirements for trainees are as follows:

- Trainees have a responsibility to protect the reputation of the BASCITT, DHSA and all placement schools' staff and pupils. Trainees must always treat fellow trainees, staff, colleagues, pupils and associates of the BASCITT, DHAS and partnership schools with professionalism and respect whilst using social networking sites.
- Social networking sites must be used responsibly, and users must ensure that neither their personal or professional reputation and/or the BASCITT, DHAS and partnership school's reputation, nor the reputation of individuals within the BASCITT, DHAS or partnership school are compromised by inappropriate postings.
- Use of social networking sites for BASCITT, DHAS and partnership school business is not permitted.
- Trainees must notify the BASCITT Programme Director and Headteacher of their placement school if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the school/setting.

- No BASCITT, DHAS or partnership school information, communication, documents, videos and/or images must be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another trainee or member of staff which could cause offence, can be posted.
- No photos or videos, which show pupils of the school who are not directly related to the person posting them, can be uploaded to any site other than the school's website.
- No comment, images or other material can be posted anywhere, by any method, that would bring the BASCITT, DHAS or partnership school or the profession into disrepute.
- Users must not contact any pupil or parent/carer on any form of social media. If a student and/or parent/carer contacts you on social media, you must immediately notify the BASCITT Programme Director, Headteacher of your placement school and Designated Safeguarding Lead.
- Users must also refrain from contacting or entering into correspondence with previous students and/or parents/carer of the partnership school in any form of social media, particularly where such contact could jeopardise the reputation of the BASCITT, DHAS, partnership school and/or members of staff.
- Users must not give pupils or parents/carers access to their social media sites e.g. being friends on Facebook. This also applies to previous pupils and their parents/carers.

Monitoring of the ICT Systems

The BASCITT may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the BASCITT's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted, and action taken in line with this policy.

Monitoring software is installed to ensure that use of the network is regularly checked by the network provider to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided.
- maintain the systems.
- prevent a breach of the law, this policy, or any other BASCITT/placement school policy.
- investigate a suspected breach of the law, this policy, or any other BASCITT/placement school policy.

Failure to Comply with the Policy

Any failure to comply with the policy will result in disciplinary action. Depending upon the severity of the offence, a breach of this policy could be considered gross misconduct and expulsion from the course.

Any unauthorised use of the BASCITT ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the BASCITT Programme Director or

Headteacher of your placement school considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The BASCITT reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

TRAINEE ACCEPTABLE USE AGREEMENT

As a BASCITT user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the BASCITT rules (set out within this policy) on its use. I will use the network/ equipment in a responsible way and observe all the restrictions explained in the BASCITT acceptable use policy. If I am in any doubt, I will consult the BASCITT Programme Director.

I agree to report any misuse of the network to the BASCITT Programme Director.

I agree to report any websites that are available on the school internet that contain inappropriate material to the BASCITT Programme Director.

I agree to ensure that portable equipment such as cameras, iPads, phones or laptops will be kept secured when not in use and to report any lapses in physical security to the BASCITT Programme Director immediately.

Specifically, when using BASCITT devices. I agree that:

- I must not use these devices for inappropriate purposes.
- I must only access those services I have been given permission to use.
- I must not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the BASCITT, DHAS or placement school network.

I understand that any failure to comply with the policy will result in disciplinary action. Depending upon the severity of the offence, a breach of this policy could be considered gross misconduct and lead to disciplinary action.

I understand that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the BASCITT will monitor communications to uphold this policy and to maintain the BASCITT network (as set out within this policy).

Signed ………………………………………………. Date ………………..

Print name ………………………………………………………………………