BHASVIC

Acceptable Use of IT Policy

For Students

Last Updated: September 2022

Review Date: September 2025

ACCEPTABLE USE OF IT POLICY

1. Policy Overview

- BHASVIC seeks to provide a stable and secure IT provision for all College users. The College IT facilities (including but not limited to, hardware, software, data, network access, third party services, online services or IT accounts) are the property of BHASVIC and are to be used in the best interests of the College.
- We are committed to protecting BHASVIC's students, staff and other stakeholders and the College itself from illegal or damaging actions by individuals, knowingly or unknowingly.
- Effective cyber security is a team effort involving the participation and support of every BHASVIC student and staff member. It is the responsibility of every computer user to know and abide by these guidelines.
- This Acceptable Use Policy is taken to include the Joint Academic Network (JANET) Acceptable Use Policy and the JANET Security Policy.
- The College also has a statutory Prevent Duty, under Section 26 of the Counter Terrorism and Security Act 2015. Prevent is a safeguarding duty to prevent young people from being drawn into being drawn into extremism and terrorism.

2. Policy Scope

- This AUP is mandatory for all users that use any sort of computing across the college. These regulations apply to anyone using the IT facilities (hardware, software, data, network access, third party services, online services or IT accounts) provided or arranged by BHASVIC.
- Users are all members of the College and all other users (staff, students, Governors, visitors, contractors and others).

3. Policy Purpose

- The purpose of this policy is to outline the acceptable use of IT facilities at BHASVIC. These rules are in place to protect users and the College. Inappropriate use exposes BHASVIC to risks including cyber-attacks, compromise of IT systems and legal issues.
- The AUP is used to make users aware of their individual responsibilities to comply with these regulations, and not to do anything on College IT systems that would conflict with the purpose of this policy.
- The AUP also explains how network monitoring will occur, and the disciplinary actions that will be used if facilities are used inappropriately.

4. Monitoring and Review of Policy

- The policy will be reviewed every annually or when changes to IT systems, or other procedures mentioned in the guidelines, make it necessary. The review will be initiated by the Assistant Principal (Digital and Communications) and the IT Network Manager who will consult with all managers with responsibilities relevant to this policy.

5. Related Documents

Internal Documents:

- Child Protection Policy and Safeguarding Procedures
- Code of Conduct (Staff)
- College Charter
- Data Protection Policy
- Dignity at Work Policy
- Disciplinary (Misconduct and Capability) Policy and Procedures
- Disciplinary Procedures for Senior Post Holders
- Equality Diversity and Inclusivity Policy
- Instruments and Articles of Governance
- Safeguarding Policy
- Social Media Policy
- Student Behaviour Policy
- Student College Contract
- Whistle blowing Policy

Advice on the College Intranet:

- BHASVIC Student Welfare – e-Safety for Learners
- BHASVIC Staff - Staff IT and e-Learning Support Area
- Email & Social Media Use - A Guide for Students
- Professional Use of Social Media - College Expectations of BHASVIC Staff

External Documents:

- Counter Terrorism and Security Act (2015)
- Combined Higher Education Software team (CHEST) User Obligations
- Communications Act (2003)
- Computer Misuse Act (1990)
- Copyright and Related Rights Regulations (2003)
- Criminal Justice Act (2003)
- Defamation Act (2013)
- Eduserv General Terms of Service
- Equality Act (2010)
- JANET Acceptable Use Policy
- JANET Security Policy
- Keeping Children Safe in Education 2016 (or most recent)
- Obscene Publications Act (1959 & 1964)
- Protection from Harassment Act (1997)
- Protection of Children Act (1999)
- Telecommunications Act (1984)

ACCEPTABLE USE POLICY

1. Access to College systems

1.1. Identity

All access to college systems must be through authorized channels, onsite or remotely, using your unique college ID. You must adhere to the College's password and multi-factor authentication processes.

- You must take all reasonable precautions to protect your IT username and password.
- You must not allow anyone else to use your IT username and password. Nobody has the authority to ask you for your password and you must not disclose it to anyone.
- You must not attempt to obtain or use anyone else's IT account, or use a device logged on under an ID which is not your own.

1.2. Passwords

- Your password must be at least ten characters in length. It must contain 3 of the 4 following characteristics:
  - Lower case letters
  - Upper case letters
  - Numbers
  - Special characters e.g. ! £ $ #
- Using three random words is a good way to create a strong, unique password that you will remember but that is hard for a hacker to guess.
- Do not use words that can be guessed (like your pet's name). You can include numbers and symbols if you need to. For example, "RedPantsTree4!"
- Your password should be unique to your college account. Do not use re-use passwords across your home and work accounts.
- If you suspect your account has been compromised, you should change your password immediately, using the "Password Reset" button on the Student Dashboard, or by contacting IT Support it.helpdesk@bhasvic.ac.uk.
- You should not autosave your password in the browser.

1.3. Infrastructure and network security

You must not jeopardise the integrity of the College IT infrastructure by, for example, doing any of the following without approval of the IT Manager:

- Damaging or moving equipment
- Reconfiguring or connecting equipment to the network
- Setting up servers or services on the network
- Deliberately or recklessly introducing malware
- Attempting to circumvent IT security measures
- Using encrypted files (unless prior written permission is obtained, and the keys or passwords made available to the IT technical support staff).

1.4. Systems and software security

The College has a legal responsibility to ensure that the software it is using has a valid licence and is being used only in accordance with the End User Licence Agreement (EULA). You must abide by software licensing terms and conditions. You should only use approved applications preinstalled on the network or on your college-owned device.

- You must not download or install any additional software (including .exe and other executable files or games) onto BHASVIC's equipment.
- Download any image, music or other large files to the network, unless related to your college work. Once work with any large file is completed, it should be deleted.
- Install, download or use any copyrighted material (such as pictures, films, music or word files), without written consent from the copyright holder or an acknowledgement of the original source of the material, as appropriate.
- Connect privately-owned laptops or other mobile devices to the network, other than through the BHASVIC eduroam wireless system (or other systems permitted at any time

by the IT Support Department).

1.5. Information

The BHASVIC network and systems are provided for you to create, view, manage and transmit data related to your college activities.

- You must not corrupt, destroy, disrupt, or violate the privacy of another User's data.
- You must not infringe copyright or break the terms of licences for software or other material.
- You must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist in nature.
- Users should be aware that the data they create on college systems remains the property of BHASVIC. You must take all reasonable steps to safeguard it and must observe the college's Data Protection policies and guidance.
- You should always log off or protect your device with screen-locking when it is unattended or not in use ('clear screen policy').

1.6. File storage

- Departments and teams are provided with SharePoint Cloud file storage, which students can access with controlled access permissions.
- Individual students are provided with OneDrive Cloud file storage to store their personal work or study-related documents.
- All data stored on SharePoint or OneDrive remains the property of the College and may be monitored, archived or deleted by the IT Support department.
- Network access rights, including access to email, SharePoint and OneDrive will be discontinued immediately when you leave BHASVIC. For students, this is 31 August at the end of their final year at college. Any files you wish to keep should be backed up in a personal file storage location prior to this date.

2. Internet, email and Social Media

2.1. Internet use

BHASVIC supports safe fair and proper usage of the Internet, and Users of the internet from college equipment or connecting to the college network must adhere to the college's policies.

- Use of BHASVIC's internet systems is intended for college use. Personal use is permitted where such use does not interfere with your college work or that of other Users. You must not:
    - Use a college computer for private use when it is needed by another student for their college work.
    - Use a college computer to play online games or use gambling sites.

  Users are accountable for their actions on internet systems.
- All internet use at BHASVIC is filtered and monitored, in accordance with our legal obligations. Monitoring data is routinely passed to the Safeguarding team for scrutiny and can be used in the event of disciplinary proceedings.
- BHASVIC may block network access to specific websites, network resources and IP addresses; ·
    - That are known to propagate malware, facilitate the compromise of sensitive or personal data or otherwise pose an information security threat ·
    - That provide or facilitate access to pornography or child abuse materials
    - That provide or facilitate access to extremism materials in relation to the College's Prevent duty.
- Staff and students wishing to view material on external websites whose access has been disabled by targeted filtering should request access through the IT Support department. Requests will be moderated by the Online Safety Group. No attempt should be made to circumvent the filters.

2.2. e-mail

The College supports safe, fair and proper use of email, for internal and external communication. BHASVIC's email system is intended for college use. Where messages are personal and private, it is more appropriate to use a personal email account.

e-mail, by its very nature, is not secure or confidential. All emails are subject to Data Protection (this applies to the sender, recipient, copied-in, subject and text sections of every email sent and received).

When you send messages outside the College your mail address identifies the College as being the mail account provider. You have a responsibility to ensure that the communications that you send do not involve the College in any potentially embarrassing or libelous situations.

College e-mail accounts are not private mail accounts, and the College has the right to access them. Students should be aware that e-mail messages sent from or to a college e-mail account can inform or be the basis of a college disciplinary procedure.

All e-mail messages sent outside the College using the College e-mail system will be automatically accompanied by the College's standard disclaimer.

All students will be given guidelines on using College e-mail accounts, College discussion forums and social network sites. For your own safety and security, you should always follow these guidelines.

Managing e-mail

- Scrutinise emails from unknown sources – alert IT Support immediately if you believe an email is suspicious. Do not open links or attachments from untrusted sources.
- All emails are subject to a system that verifies them for audit and legal purposes.
- Emails are subject to automatic archive and deletion according to our Data Retention policy.

2.3. Social Media and Blogging

Social media forms a large part of modern communications, and the College recognizes the benefits that effective use of these tools can bring. You must ensure that you are aware of your obligations when using social media either personally or for work regardless of on college equipment or not, and the potential consequences of unacceptable use of social media.

Student use of social media

BHASVIC Students using any form of social media should follow this basic principle – **Be Professional, Responsible and Respectful**

You must:

- Adhere to the terms and conditions of your Student Contract when using social media, specifically the fourth fundamental obligation, namely "You should always show consideration to those members of the BHASVIC community, including the online community, you come into contact with. Your interactions should be polite, and you should actively respect the environment in which we all work. You are ambassadors for the College and are responsible for how your behaviour and language impacts on the good reputation of the College. These expectations apply both on and off-site and on and off-line, including comments you post about BHASVIC via social media."
- Be accurate, fair and transparent when creating or altering online sources of information.

You must not:

- Engage in activities involving social media which might bring BHASVIC into disrepute
- Represent your personal views as those of BHASVIC on any social medium
- Discuss personal information about students or staff at BHASVIC on College social media sites
- Use social media and the internet in any way to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations or BHASVIC.

3. Bring Your Own Device (BYOD)

3.1 BYOD

Bring Your Own Device (BYOD) means accessing College systems and information through personally owned devices, such as tablets, smartphones, laptops and PCs. We encourage students to acquire and use their own laptop for college study.

We recognize the benefits of being able to use personally owned devices such as smartphones, tablets, laptops and home PCs to access college systems and information, but it is important that students follow

this policy carefully to ensure that college information security is not compromised.

- The college is fully committed to ensuring that the principles of the AUP and DPA are adhered to, regardless of whether the user is accessing data on a college owned, or personally owned, device. Any college data accessed or stored on a personal device is owned by BHASVIC.
- All other College policies and procedures apply in the context of BYOD.
- Users must undertake to ensure that the personal device/s:
  - Have the most recent operating system update installed
  - Have up-to-date anti-virus software installed and running
  - Accept all software updates
  - Are not modified in any way outside manufacturer guidelines
  - Are secured with a strong password and preferably Biometric Authentication (face or fingerprint recognition)
  - Are set up with an auto-lock (device locks automatically after an idle time period)
  - Are not cached to remember passwords
  - Users must not save any college-owned data which may be considered personal, sensitive, confidential or of commercial value to personally owned devices.
- The College provides information systems such as college email, website, VLE, Capita Advantage and O365, which allow secure access to data using an internet browser. When accessing these systems using a personally owned device, users should ensure that they log out at the end of the session.
- The College reserves the right to clear data stored on any personally owned device which has been used to access College data. This may also result in the removal of any personal data stored on the device.
- It is the individual student's responsibility to ensure that you have backups of critical work in case of accidental loss of your files.

3.2 Data transfer and storage

- Users must not transfer any College-owned data which may be considered personal, sensitive, confidential or of commercial value to personally owned devices.
- The college provides Cloud-based storage in SharePoint and OneDrive, which can be accessed both inside and outside college, for the storage of college data.
- Users should disable automated, cloud hosted, back-up services on any personal device which is used to access sensitive college data.
- Users should clearly separate personal usage and college usage on any BYOD device.

3.3 Device security

- The college takes no responsibility for the maintenance, support or costs associated with personally owned devices.
- Users must set up remote wipe capabilities, which ensure that the device can be 'wiped' of all data in the case of loss or theft.
- Users must securely remove all College data when their contract with the College ends.

3.4 Wireless network

- The college offers a logged wireless service (Wi-Fi) for users. Connection to the college wireless network requires a valid username and password. All college Wi-Fi users must agree to adhere to the Acceptable Use Policy.
- Users (staff, students and visitors) connecting a personal device to the college Wi-Fi must use the eduroam service provided. Personal devices must not be

physically connected (using an ethernet connection) to the college network.

- Users must not attempt to breach the security or filtering measures of the college network. Users must not download illegal software via this network. If downloading content from the internet, it is the responsibility of the user to ensure that they adhere to the requirements of the publisher, as well as copyright laws.

4. Monitoring and filtering

4.1. Network Monitoring

BHASVIC monitors and records the use of its IT services at both client and infrastructure levels. All college accounts are the property of the college and are subject to automated monitoring and web filtering.

- For information security purposes, telephone and computer systems (including email and online communication platforms such as Teams), and any personal use of them, may be continually monitored by automated for the purposes of
  - The effective and efficient planning and operation of the IT facilities
  - Detection, mitigation and prevention of cyber security threats
- Further targeted monitoring will be carried out if justified for the following purposes:
  - Detection and prevention of infringement of these and other policies and regulations
  - Investigation of alleged misconduct
  - To comply with any legal obligation

4.2. Filtering

The college uses automatic web filtering to block network access to specific websites, network resources and IP addresses:

- That are known to propagate malware, facilitate the compromise of sensitive or personal data or otherwise pose an information security threat
- That provide or facilitate access to child abuse materials, in line with the college's Safeguarding policy
- That provide or facilitate access to extremism materials in relation to the college's Prevent duty

Staff and students wishing to view material on external websites whose access has been disabled by targeted filtering should submit their request to IT Support. No attempt should be made to circumvent the filters.

4.3. Training

Students will receive training in digital identity and citizenship through the tutorial programme.

Each time you log on to the College Network you will confirm that you accept the Acceptable Use Policy. In agreeing to this policy, you are consenting to it. In addition, the College wishes to make you aware that Close Circuit Television (CCTV) is in operation in the College for the protection of employees and students.

5. Precautionary and disciplinary actions

- Excessive private access to the Internet from College computers may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. The sites accessed by you must comply with the restrictions set out in these guidelines.
- IT Technical Staff can at any time temporarily remove a User's access to the network or delete files if any unacceptable use has been made or is suspected. If an investigation confirms that the Acceptable Use Policy has not been followed, the User

may be permanently barred from accessing the college IT facilities.

- Serious misuse will be referred to the Assistant Principal (Digital and Communications) who may initiate the college disciplinary procedures. Inappropriate use of the College systems is seen as misconduct and will, in certain circumstances, be treated by the College as gross misconduct. The College reserves the right to use the content of any e-mail or files in a student's area in any disciplinary process.
- In some cases, the College may be legally obliged to contact the police or other authority if the incident warrants it.
- In addition, the BHASVIC network is part of a larger network community called JANET. The College is responsible for users conduct on this network and will implement disciplinary action if our standing as a member is compromised.

6. IT Technical Support

The IT technical support staff are there to assist you. If you require further information or help about the use or set up of your computer, or have worries about the security of your work, you should contact any of the IT technical support team in Room 126 or via it.helpdesk@bhasvic.ac.uk.