BHASVIC

ACCEPTABLE USE OF COLLEGE IT POLICY ~ STUDENTS

Last Updated: JULY 2017

Review Date: JULY 2020

ACCEPTABLE USE OF THE COLLEGE IT NETWORK POLICY

1. Policy Statement

- The College seeks to provide a modern, stable and secure IT network for all College users at all times.
- The College expects users of College IT systems to use them appropriately so that a good service can be maintained.
- As part of our service, elements of our network are open to the internet through email and web interfaces. We expect users to conform to relevant legal responsibilities and not to bring the College into disrepute.
- 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 duty, under Section 26 of the Counter Terrorism and Security Act 2015, termed "PREVENT". The purpose of this duty is to aid the process of preventing people being drawn into terrorism.

2. Policy Scope

- Members of the College and all other users (staff, students, Governors, visitors, contractors and others).

3. Policy Purpose

- To protect the College IT systems from intentional or unintentional abuse. This may otherwise lead to a reduction or denial of service to all College users.
- To uphold the legal responsibility on the part of the College to ensure that all users of College IT systems work within the requirements of the relevant Acts, Regulations and Laws detailed in Section 5 – "Related Documents" below.
- To try to prevent any activity on the College IT networks that could bring the College into disrepute or cause financial or legal penalties.
- To make users aware, through provision of a detailed set of advice and guidelines attached as appendices to this policy and on the College network, of their individual responsibilities to ensure that they do not do anything on College IT systems that would conflict with the purpose of this policy.
- To detail within those guidelines how network monitoring will occur and the range of disciplinary actions to be used if the systems are used inappropriately.

4. Monitoring and Review of Policy

- The policy will be reviewed every three years or more frequently if necessary. The review will be initiated by the Assistant Principal (Director of Resources) and the IT Network Manager who will consult with all managers with responsibilities relevant to this policy.
- The attached appendix containing advice and guidelines will be reviewed annually and at other times when changes to IT systems, or other procedures mentioned in the guidelines, make it necessary. The College may make such variations to these procedures as it sees fit, subject to informing network users and normal principles of reasonableness and fairness.

5. Related Documents

Internal Documents:

- Bullying and Harassment Policy (Students)
- Child Protection Policy and 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 Discipline Policy and Procedures
- The Student College Contract
- Whistle blowing Policy

Advice on the College Intranet:

- BHASVIC Student Welfare – E- Safety for Learners
- BHASVIC Staff - Staff ILT 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)

APPENDIX TO THE ACCEPTABLE USE OF THE COLLEGE IT NETWORK POLICY – STUDENTS

ADVICE AND PROCEDURES

The following is intended to provide students with clear advice and guidelines about how they may use the College IT facilities.

1. Section One –Network Use and Security

1.1. Network Security

You must be a currently registered student with a designated ID to use the BHASVIC network.

You must not

- Reveal your network password to anyone or allow any other user to use a machine that is logged in under your name (see password security guidance below)
- Use any ID which is not your own, or use a machine which is logged on under an ID which is not yours
- Corrupt, destroy, disrupt or violate the privacy of another user's data or work
- Introduce viruses or other disruptive elements to the system
- Use encrypted files (unless prior written permission is obtained and the keys or passwords made available to the IT technical support staff).

Password Guidance:

- You should have a password that is not a name or a complete word, nor a common abbreviation. Use eight letters / numbers or more.
- You must take care not to leave computers logged in under your user ID, which would allow other users or students to access the network in your name.
- Passwords should not be auto saved when using public computers.
- Change your password regularly (you will periodically be prompted to do so by the system). Do not write your password down.
- It is advisable to reset your password before holidays to ensure that it does not expire – which would prevent access to the VLE and your files from home. If you forget your password it can be reset by IT Technical Support.

1.2. Network Usage

You may use the BHASVIC network and computing resources to create, view and transmit work relating to your College activities. Network access rights and saved files will be deleted when you leave the College, so you should not keep files on the network that you will need once you have left.

You may not at any time create, intentionally view or transmit any images, literature or other data that:

- Are offensive, obscene, indecent or defamatory
- Are designed or likely to cause annoyance, inconvenience or needless anxiety – e.g. bullying or harassment of students, staff or others by email or other means.
- Infringe the copyright of another person

File quota

A file quota is the size of documents that a user can store on the file server (N: drive).

The College will limit the size of files an individual can leave on this file server. For this reason, document areas should be regarded as only a temporary repository for files and a location to store personal work related files. The following limits will apply to files:

- Student document drive (N) – 750 MB

In addition the college will provide all students with a One Drive (Office365) storage of 10 GB which can be used to store college files.

The user is responsible for the content and maintenance of their network drive.

Remember:

- Check periodically and remain within your disk quota.
- Keep files stored in your network drive to a minimum

Archiving and deletion of files

- Files older than a year will be subject to automatic archive.
- Files will be kept for 1 year after completion of a student's studies at college, after which they will be subject to automatic deletion

1.3. Systems and Software Security

You may:

- Only use applications preinstalled on the network, on the workstation or on College supplied media.
- Use writeable media, USB Memory Cards and e-mail attachments with the College workstations to transport files to, and from home or around the College, although you must ensure files are virus free and compatible with the College systems. You must be aware that the College antivirus system may automatically delete infected files.

You may not: (unless you have been guided as part of your College course)

- Interfere with the software or hardware configuration of networked equipment or systems in any way.
- Install, download or use any additional software (includes .exe and other executable files and games).
- Install, download or use any images, music or other large files without specific permission from your teacher or IT Support. Once work with any large file is completed they 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 personal laptops or other mobile devices to the network, other than through the eduroam wireless system.

2. Section Two - Internet, e-mail and Social Media Use

2.1. Internet use

The Internet is a valuable tool for your College work.

Reasonable private research on the internet is allowed if it does not interfere with your College work, however you must not:

- Take up a workstation which is required by other students for their work (eg at peak times in the Library)
- Play online games or use gambling sites

All users of the network have their internet use automatically monitored and a record of sites visited is recorded by IT technical support.

2.2. e-mail Use

The College arranges for every student to have an email account which is administered for the College by Microsoft (Office365) (including setting filters for viruses and spam mail etc.).

- 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.**
- Students should be aware that the College may access or remove these accounts at any time as they are not your private email account. Misuse of e-mail messages sent from or to these e-mail accounts can inform or be the basis of College disciplinary actions.
- These email accounts will remain live for one year after which they will be deleted. These accounts can be converted to alumni accounts on request to IT Support.
- 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 follow these guidelines at all times.

2.3 Social Media Use

Principles for Students– Be Professional, Responsible and Respectful

- You should:
  - maintain the terms and conditions of your Student Contract when using Social Media, specifically the fourth fundamental obligation, namely "You should at all times show consideration to those members of the BHASVIC 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." *In this instance the community also includes the online community
  - be accurate, fair and transparent when creating or altering online sources of information.

- You should 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.

Excerpt from Social Media Policy (September 2017)

3. Section Three -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.

- Traditionally, College systems and information were accessed almost exclusively through College-owned devices, but the rise in the popularity of smart technology means that this is no longer the case.
- The College recognizes the benefits of a flexible BYOD approach. However, BYOD must be carefully managed to ensure that standards of information security are not compromised.
- The College seeks to promote the effective and safe use of information systems to ensure a productive environment for learning, teaching and work. The College is responsible for the data which it holds and manages that data in accordance with the Acceptable Use Policy (AUP), the Data Protection Policy for Staff and Students, and the Data Protection Act 1998 (DPA).
- The Data Protection Act sets out the 8 principles of good information handling and clearly sets out the responsibilities for those storing and handling information. BHASVIC is responsible for the personal information which it holds. A full overview of the Data Protection Act (DPA) and the College's associated responsibilities can be found in the Data Protection Policy for Staff and Data Protection Policy for Students.
- 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 stored on a personal device is owned by the College.
- All other College policies and procedures apply in the context of BYOD.
- 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 Myfiles, 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.
- 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.
- Users should disable automated, cloud hosted, back-up services on any device which is used to access College data.
- Users should clearly separate personal usage and College usage on any BYOD device.

3.2 Data transfer

- Users must not transfer any College-owned data which may be considered personal, sensitive, confidential or of commercial value to personally owned devices.
- Any College data transferred via a USB drive should be securely deleted from the USB drive once the transfer is complete.
- Cloud storage services are third-party organisations that allow the user to back up files to the internet, which facilitates access from any internet-enabled device.

Cloud storage providers include, but are not limited to; Dropbox, OneDrive, Google Drive and iCloud. Users should be fully aware that data stored within these services is being held by a third party. However, ownership of the College data remains with the College and responsibility for data security remains with the user.

3.3 Device security

If personal devices are used to access College data, users must ensure that they are:

- Up to date with anti-virus software
- Up to date with the latest software updates
- Not modified in any way outside manufacturer guidelines
- Secured with a strong password or passcode
- Set up with an auto-lock (device locks automatically after an idle time period)
- Not cached to remember passwords

The College takes no responsibility for the maintenance, support or costs associated with personally owned devices.

Loss, theft or disposal of device

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 relationship with the College ends.

3.4 Wireless network

The College offers a logged wireless service (wifi) for users. Connection to the College wireless network requires a valid username and password (the same details you use to log in to any College computer). By using the College wireless network, all users agree to adhere to the Acceptable Use Policy.

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.

Users must not physically connect any personally owned device to the College network without prior agreement with IT Support.

4. Section Four- Maintaining Standards

4.1. Network Monitoring

Computer accounts are the property of the College and are designed to assist in the performance of your work. You should, therefore have no expectation of privacy in any of your stored work.

The College has the right to monitor any and all aspects of its telecommunication and computer systems that are available to you, and to monitor, intercept and/or record any communications made or received, including telephones, email or Internet communications. When logging on to the College Network you will confirm that you accept the Acceptable Use of Computers 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.

BHASVIC IT Technical staff may:

- Monitor activities on the network, as appropriate, to ensure that the resources are not compromised or the

College reputation brought into disrepute.

- Check the files that any user has in their area at any time, or view activities in progress either directly or remotely to ensure compliance with the Acceptable Use Policy.

All BHASVIC staff may ask a student to explain their activities on a computer at any time, if they believe that the use may be inappropriate according to this policy and guidelines.

Storage quotas are applied to all network accounts. You are advised to remove all large and unwanted files as soon as possible after using them so that you do not take up unnecessary space on the system. Once you reach your quota, the system will not allow work to be saved until you have cleared sufficient space.

4.2. Precautionary and Disciplinary Actions

For the protection of the integrity of the Network:

- IT Technical Staff can at any time temporarily remove a user's access to the network if any unacceptable use has been made or is suspected.
- IT Technical Staff may remove files from user areas if they believe that unacceptable use has occurred.
- If any student user is found to have contravened this policy they will have their access to the network removed until the student has discussed the misuse with IT Technical staff.
- Misuse will be dealt with under the college disciplinary system by IT Technical staff. Appropriate actions will be taken according to the level of misuse
- 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.

4.3. Backups and IT Technical Support

Although security of the Network is maintained and backups of your area are taken regularly, it is <u>your</u> responsibility to ensure that you have your own backups of critical work in case of loss of your files due to accidental erasure.

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 the College online Helpdesk.