BHASVIC

ACCEPTABLE USE OF THE COLLEGE IT POLICY - STAFF

Last Updated: JULY 2017

Review Date: JULY 2020

BHASVIC

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 – STAFF

ADVICE AND PROCEDURES

The following is intended to provide staff 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 user 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). This does not include password protected files.

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 staff network in your name.
- Passwords must 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
- Unsolicited commercial or advertising material

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:

- Staff document drive (N) - 5GB

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 older than 4 years 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:

- 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 to the network any image, music or other large files, unless related to your College work. 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 BHASVIC "Guest" wireless system or other systems allowed at any time by the IT Support Department.

PCI-DSS Compliance

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety.

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

2.1. Internet use

Reasonable private use of the internet from College computers is permitted but should not interfere with work. Excessive private use may lead to disciplinary action and may in certain circumstances be treated by the college as gross misconduct.

Users may not access, encourage access or disseminate materials which the College management deems to be obscene, pornographic, excessively violent, offensive or that acts as an incitement to criminal behaviour. If a specific project is being worked on that would result in this material being necessary, then permission should be sought from line management. However, it should be emphasised that this permission will be denied if access would contravene the law.

All users of the network have their internet use automatically monitored and a record of sites visited is recorded by the IT team. This information can be used in the event of disciplinary proceedings.

2.2. e-mail Use

e–mail provides a valuable function within any professional establishment. It is recognised within BHASVIC as an appropriate way of communicating information internally and externally. This includes enabling messages to be seen by people other than the original recipient. It also enables contact to be

made outside of the College and for items such as agendas, minutes, and work documents to be sent as attachments between people. It does not replace face to face contact with other members of the College. For this reason the college supplies its staff with a college e-mail account. All users should be clear that this does not serve the same function as a private mail account.

Where messages are personal and private, a private e-mail account is the more appropriate vehicle to use.

As part of professional responsibility, staff should regularly check their mail account and respond as appropriate. Some messages will require a timely response so that delays and disruptions to other people's work can be avoided. There is a College expectation that e- mail accounts should be checked by staff at least every 24 hours (excluding periods when staff are not in college (e.g. holidays). Part-time staff who have a timetable that prevents this should ensure that they check their e-mail accounts on the days that they are in college.

e-mail, by its very nature, is not secure or confidential. Messages are not private and can be seen by other people. Do not put anything in a message that should not be seen by everyone. Legally, the laws of libel apply.

College e-mail accounts are not private mail accounts and the College has the right to access them. Staff 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 accompanied by the College's standard disclaimer automatically.

Writing a mail message

Staff are expected to exercise discretion with the amount of mail sent and be aware of the following advice on sensible usage:

- Keep mail messages short and to the point.
- The size of email attachments should be kept to a minimum.
- Do not use the College email service for private adverts, requests, publicity etc. this uses up valuable network space and is annoying to other users.
- Use the subject heading to identify what your message is about.
- View email as an open postcard. Your mail message should be authored with this in mind - an open communication that anyone should be able to read.
- When you send messages outside of 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.**

e-mail manners

- Think carefully about what you are sending. It is easy to be misinterpreted unless you have made it very clear what you are trying to say. Readers of e mails cannot see your face or hear your tone of voice so all expression is derived from your words and punctuation.
- Do not use e-mail as a medium for initiating or prolonging a disagreement. If you have a problem with another member of the College then resolve the situation face to face.
- If you read something that offends you, do not respond immediately. It may not have been intended to offend. Take time to calm down, reread and respond without being offensive only if you consider it worthy of response.
- Do not use e-mail to forward on jokes/ funny web sites/ attachments etc. The recipient may find these irritating and even offensive.
- Respect other e-mail users. Do not use e-mail as a replacement for meeting someone or for trivial enquiries that can be easily answered with some effort on your part.
- Do not bombard people with mail messages. It quickly becomes tiresome if you have to answer large numbers of messages every day, most of which can be dealt with face to face that day.
- Use distribution lists carefully. Only send messages to those who need to receive them e.g. do not use the "All Staff" group when the message is only aimed at selected staff.

Managing Incoming e-mail

- Do not open emails or attachment from unknown or untrusted sources
- Delete mail messages as soon as they are no longer needed. (Note – Outlook settings can be altered to automatically delete messages in the deleted items folder after a period of time. This

can be set within the tools menu. Please ask IT Support for help if you wish to set delete options).
- Store useful messages in folders and check these regularly to identify any that can be deleted.

Archiving and deletion of e-mails

- All emails are subject to a system that verifies them for audit and legal purposes.
- Email older than a year will be subject to automatic archive.
- Email older than 3 years will be subject to automatic deletion.

Social Media

Guidelines for Social Media
Social media can be useful as a way of keeping in touch for College activity. To ensure a positive online environment for students and staff, the following code of conduct has been produced to which all college social media participants should adhere to:

- You are legally liable for anything you write or present online. Employees and students can be disciplined by the College or sued by College employees, competitors and any individual or company for any commentary, content or images that are viewed as defamatory, pornographic, proprietary, harassing or that can create a hostile work environment.
- No written comment should be made that could be offensive to anyone in any of the seven
- Equality and Diversity strands: race and ethnicity, age, disability, gender, gender identity, sexual orientation, religion or belief. In addition, no written comment should be made that could be offensive towards any nationality or socio-economic group.
- You are posting content onto the World Wide Web and cannot ensure who does and does not have access to your information.
- Information you post online may continue to stay on the World Wide Web even after you erase or delete that information from pages.
- Before participating in any online community understand that anything posted online is available to anyone in the world.
- Do not post information, photos or other items online that could reflect negatively on you, your family or the BHASVIC community.
- Be discreet, respectful, gracious and as accurate as you can be in any comments or content you post online.

Staff are also referred to the Safeguarding Policy which reminds them that they have a responsibility to promote the wellbeing and safety of our students. This would include any form of personal conversation or comment through the medium of the Internet. Staff should:

- Maintain separate personal and professional social media accounts (such as that of Facebook or Twitter) and only use the professional account in communications with BHASVIC students.
- Not establish or seek to establish social contact with students for the purpose of securing a friendship or to pursue or strengthen a relationship via their professional account.
- Set-up group work under the College identity, or using an existing College account (for example, by using the department"s social media site if there is one, or by using the BHASVIC logo, and this policy and procedures to set up a new sharing hub, forum or networking account on Twitter, Facebook, YouTube, etc.).
- Ensure that the appropriate privacy settings are in place to protect the identity of all students who use any College generated social media accounts.

Guidelines for Blogging
If staff and / or a student own a blogging site the following guidelines should apply:

- Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author's alone and do not represent the views of the College. Be clear and write in first person. Make your writing clear that you are speaking for yourself and not on behalf of the College.

- Information published on your blog should comply with the College policies. This also applies to comments posted on other blogs, forums and social networking sites.
- Be respectful to the College's other employees, students and competitors.
- Social media activities should not interfere with work commitments.
- Your online presence reflects the College. Be aware that your actions captured via images, posts, or comments can reflect that of the College.
- Do not reference College employees or partners without their express consent.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- College logos and trademarks may not be used without the written consent of the Marketing Department.

Activities not covered above

- Where no guidelines exist, staff should use their professional judgement and take the most prudent action possible. Consult with the College's Marketing Manager if you are uncertain.
- Media contacts about the College, our students, employees, partners, customers and competitors must be referred for co-ordination and guidance to the Marketing Manager.
- Please note that any activity on College's internal systems are monitored and recorded. Any external web activity is monitored, recorded and filtered.

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 should 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 any other user, at any time, to explain their activities on a computer, if they believe that it is not work related, or if the work falls outside of acceptable use guidelines. Staff can report behaviours that they think inappropriate under the normal complaints or whistle blowing policies.

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:

- 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. Accessing inappropriate sites may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct, (this is as defined in the Gross Misconduct section of the Disciplinary Policy).
- 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 unacceptable use has been made or is suspected, the user's line manager will be informed. IT technical staff may then remove user's access to the network and remove files from user areas if an investigation confirms that the acceptable use policy has not been followed.
- Serious misuse will be referred to the Assistant Principal (Director of Resources) 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 an employee'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.

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.