

# **ACCEPTABLE USE OF COMPUTERS POLICY**

Last Updated:  
Finance & General Purposes Committee:  
Corporation Approval:  
Review Date:

March 2009  
March 2009  
March 2009  
Every 3 Years





## ACCEPTABLE USE OF COMPUTERS POLICY - STAFF

The following document is intended to provide staff with clear guidelines about how they may use the College IT facilities.

The guidelines set out the individual responsibility of all staff to ensure that they do not do anything on networked equipment that constitutes an abuse of the College network systems or networked resources (including the time of outside agencies that may be involved with BHASVIC). This includes any activity that could bring the College into disrepute or cause financial or legal penalties.

In addition to this the guidelines ensure the legal responsibility on the part of the College to ensure that all users of IT within the College are working within the requirements of the following acts: Obscene Publications act (1959), Protection of Children Act (1978), Criminal Justice Act 1988, Protection from Harassment Act 1997, Defamation Act 1996, Computer Misuse Act 1990, Telecommunications Act (1984) and Communications Act (2003); in addition to the Copyright and Related Rights Regulations 2003 and the Discrimination (age, sex, race, disability, sexual orientation and religion or belief) and Contract Laws. The ACAS guide to legal considerations in internet and email policies (at [www.acas.org.uk](http://www.acas.org.uk)), gives brief information on how these acts may impact on employers, staff and students.

### 1. Section One – The Network Use and Security

#### 1.1. Network Security

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

You must not deliberately:

- Reveal your network password to anyone
- Allow any other user to use a machine that is logged in under your name
- 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
- Use BHASVIC resources in a way that denies service to other users
- 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 Security

- Do not write your password down.
- Change your password regularly (you will periodically be prompted to do so by the system). If you do happen to forget your password it can be reset by IT Technical Support.

#### 1.2. Network usage guidelines

You may use the BHASVIC network and computing resources to create, view and transmit work relating to your college activities. You must ensure care where computers are in open access environments that other users do not access the network through leaving the computer logged in under your user id.

You may not at any time create, intentionally view or transmit any materials that are:

- offensive, obscene or indecent images, literature or other data
- designed or likely to cause annoyance, inconvenience or needless anxiety
- defamatory
- infringe the copyright of another person
- unsolicited commercial or advertising material

### **1.3. Systems and Software Security**

You may:

- only use applications preinstalled on the network, on the workstation or on BHASVIC supplied CD-ROMS.
- use floppy disks, writeable CDs, USB Memory Cards and e-mail attachments with the College workstations to transport files to, and from home, 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 to function on the College network and associated equipment (includes screen savers, MSN messenger, wallpaper and games) without prior permission.
- Install, download or use any copyrighted materials, without written consent from the copyright holder.
- Connect non-BHASVIC laptops or PDA's to the network or to the College telephone system, unless permission is obtained from a member of the IT Technical Staff.
- Connect any extra hardware to individual machines, except with prior permission.

### **1.4. 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. 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 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 this Acceptable Use Policy.

All BHASVIC staff may ask any 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.

## **Section 2 - Internet / e-mail use and guidelines**

### **1.5. Internet Use**

Reasonable private use of the internet is permitted but should not interfere with work. Excessive private use during working hours 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.

Staff are required to ensure the following:

- Files containing copyright protected material must not be downloaded, forwarded or transmitted to third parties without the permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.
- Copyrighted software must never be downloaded.
- Large files should not be downloaded unless absolutely essential – and these are deleted as soon as possible thereafter.
- Do not import executable files on to the College's system without having them scanned for viruses, e.g files with a name that ends in .exe.

### **1.6. e-mail use and guidelines**

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 a more appropriate vehicle.

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 and 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 accompanied by the College's standard disclaimer automatically.

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

Staff are required to ensure the following:

- The size of email attachments should be kept to a minimum.
- Do not open emails or attachment from unknown or untrusted sources

Writing a mail message

- Keep mail messages short and to the point.
- 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 libellous 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 faces or hear your tone of voice so all expression is derived from your words and punctuation. Remember, the use of capital letters could indicate shouting.
- 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. Remember the Trust Culture within which we work.
- 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 e-mail

- 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 an IT technician 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.

## **2. Section 3 - Disciplinary Actions**

Excessive private access to the Internet during working hours 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).

If any unacceptable use has been made or is suspected, the user's line manager will be informed. I.T. 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 Vice Principal and 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.