E-Mail & Internet User Policy for Governors, Staff & Students (Acceptable Use Policy) 2018-21

Purpose of Policy/ Document

This document aims to clarify and stipulate the correct usage of Governor, staff and student electronic communications (including email and internet use) whilst off and on college premises and/or using college equipment.

Application of Policy (Range and Scope)

This document applies to all users (including visitors and guests).

Particular Legal Requirements/Issues Outside of Equality, Diversity and Disability (E.D.D)

Links with Other Policies/Documents

Professional Code of Standards for Staff
Student Standards
Data Protection Policy (GDPR)
Safeguarding Policy
Social Media Policy

Equality, Diversity and Disability (Disability, Equality, Duty Impact Assessment)

Has a Preliminary Equality Analysis been completed?
Yes **Date Completed: 20/04/2015**

Is a full Impact Assessment required?
No

If 'yes', has a copy been sent to the Equality Manager?
N/a

POLICY REFERENCE	**EMP35**
CATEGORY	**Employment**
AUTHOR / ORIGINATOR	**VP Corporate & Resources**
ISSUE DATE	**Sept 2018**
REVIEW DATE	**Sept 2021**
POSTHOLDER RESPONSIBLE FOR REVIEW	**VP Corporate & Resources**
RATIFIED /AUTHORISED BY	**SLT**

E-MAIL AND INTERNET POLICY

1. Introduction

The provision and use of E-Mail and the Internet in the College opens up opportunities for marketing, communication and research but it may also create unforeseen consequences and problems. E-Mail can boost efficiency through improved communication, and internet use may stimulate creativity; facilitate research and the gathering of information, however both can also offer opportunities for misuse.

It is important that College Governors, staff & students are aware of the guidelines that they are expected to follow in using E-Mail and the Internet. The College's policy is set out below to ensure that users understand how the system should be used. In this policy users are made aware of the possible dangers of using the system and the fact that disciplinary action may result from its misuse.

The policy attempts to achieve a balance between allowing user's access to E-Mail and Internet services to assist in their work and studies whilst addressing, as far as possible, the risks of such access.

It is therefore essential that users read and agree to be bound by these guidelines and make themselves aware of the potential legal liabilities involved in using E-Mail and the Internet.

2. General Points

2.1 Use of E-Mail and the Internet is primarily for work or study related purposes.

2.2 The College is the owner of the E-Mail and Internet communication resources. These are designed to assist in the performance of your work, and your studies. You should, therefore, have no expectation of privacy in any E-Mail sent or received, whether it is of a business/course related or a personal nature and in view of the range of legal liabilities that can arise from users having access to E-Mail and the Internet, the College may monitor and intercept communications as considered necessary within legislative requirements.

2.3 The College accepts that there are occasions when Governors, staff and students will receive unsolicited material of an obscene or offensive nature. However you should note that under this procedure improper use of E-Mail and the Internet by users to knowingly access, download or transmit any material which might reasonably be considered to be obscene, abusive, sexist, racist or defamatory could, in certain circumstances, be treated by the College as gross misconduct., or result in students being excluded from their course, or from the College. You should be aware that such material may also be contained in jokes sent by E-Mail. The College reserves the right to use the content of any E-Mail in any disciplinary process.

3. Use of E-Mail

3.1 E-Mails should be drafted with care. Due to the informal nature of E-Mail, it is easy to forget that it is a permanent form of written communication and that material can be recovered even when it is deleted from your computer. As such users must take reasonable care in ensuring that E-Mails are constructed so as not to cause annoyance, inconvenience or needless anxiety.

3.2 Users should not make defamatory remarks in E-Mails about Governors, staff, students,

competitors or any other person since written derogatory remarks can constitute libel.

3.3 Users should regularly read and delete unnecessary E-Mails to prevent over-burdening the system. Regular deleting of items in Inbox and Deleted Items will enable the system to work effectively.

3.4 Whilst E-mail is primarily for college related use, reasonable private use of E-Mail is permitted. The "AllStaff" & "AllStudents" E-mail addresses **must not** be used for personal reasons (e.g. personal events, sale of goods, personal or political views), and the contents of personal E-Mails must comply with the restrictions set out in these guidelines.

3.5 By sending any electronic communications via the College's IT systems, you are explicitly consenting to the processing of any personal data contained within. If you do not wish the College to process such data you should communicate it by other means.

3.6 The 'All Staff' E-mail address is for internal use only and must not, be given to third parties.

3.7 Be security conscious. The Data Protection Act requires that adequate security is maintained to protect personal information held on e-mails, related archives and software (see appendix 1). Do not allow anyone to use your network log-on and password, and do not leave your network account logged on when you have walked away from the computer without ensuring you have locked the computer to prevent others accessing your account.

When working and transmitting documents that contain personal or sensitive information outside of the College, those documents should always be encrypted. The passwords for subsequently decrypting the documents should not be sent by the same transmission media, *.i.e.* if you are emailing an encrypted document, do not include the password to decrypt that document via email. If you require assistance with encryption, please contact the College's IT Support team.

NB. You must always keep an unencrypted copy of the document in a secure location on the College Computer network.

3.8 Under no circumstances should bank or credit / debit card information be included on emails.

3.9 When an employee, volunteer, or governor leaves the College's employ an E-Mail will be generated from H.R. to I.T. who will then disable (*not delete*) the individuals account with immediate effect (*unless instructed differently by a member of the Executive, or Head of HR*).

3.10 When a student leaves the College at the end of their course their account will be disabled two calendar weeks after the official course end date. Where a student has their enrolment terminated prior to the course end date, the I.T. Department will disable the account with immediate effect (*This will initially be confirmed in an E-Mail to IT Services from the relevant CRQ Director or Leader*).

3.11 **All** E-Mails sent to an individual using the howcollege.ac.uk address after a user account has been disabled will be returned to the sender. After a period of three (3) years all remaining E-Mails relating to the former user will be deleted. If access is required to an individual's mailbox or home directory by any other user a Mailbox / Home Directory Access Request must be submitted via the College Portal.

3.12 The College may provide secure E-Mail and Internet access for recognised Trade Unions. These will be provided on the understanding that the facilities are used in connection with normal trade union activities. If there are grounds to believe that the site or address are being

abused then the matter will be referred to the Union full time official in order to agree access for the purposes of investigation.

4. Use of the Internet

4.1 Computer and internet access is provided to all users on the understanding that it will be exercised in a responsible manner, for educational purposes and College business use.

4.2 In addition Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on Schools, Colleges, Universities and Local Authorities in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism", with section 8 of the policy stating:
In order to safeguard students utilising the IT facilities at the College and prevent individuals accessing extremist materials via the College's network, we will ensure:
8.1 The organisation will retain the ability to log and retain records of all electronic communications (web browsing, e-mail traffic etc.) by users on the College network.
8.2 Appropriate staff will be available to monitor any aspects of its telephony network, including mobile phones and any computing facilities made available to staff, students and visitors.
8.5 All unusual and/or suspicious events including breaches of security are to be reported immediately via the Safeguarding Team for further investigation.'

4.3 In support of this the College uses monitoring software which will take a screenshot of what is currently being displayed on the computer screen if:

1. It detects a target keyword or phrase has been typed.

2. Analysis of images or video displayed on a screen identifies something that could be viewed as pornographic.

These screenshots are then used to identify any potential Safe Guarding and/or Prevent concerns. A scheduled report containing Usernames, Date\Time and Location will be generated identifying any concerns.

The monitoring is multi-lingual (including script or character based languages) and enacted against <u>all activity</u> on the computer, not just web based work, and that all captured screenshots are retained for the duration the user account is active at the College. This retained information is used to contextualise and spot trends. Monitoring will continue even when the equipment is not attached to the Internet, whether via the College's or another network.

4.4 Some group study areas may incorporate the use of additional remote monitoring tools to ensure these standards are met, where implemented signage will indicate this in a clear and understandable manner.

4.2 All sites accessed by users must comply with the restrictions set out in these guidelines and the social media policy. The creation or transmission (*other than for properly supervised and lawful research*) of any offensive, obscene or indecent images, data or other material may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct, or result in a student's exclusion from their course and/or the College.

4.3 Copyright applies to all text, pictures, video and sound, including those sent by E-Mail or on the Internet. Files containing such copyright protected material may 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.

4.4 Copyrighted material must never be downloaded/uploaded without the clear consent of the copyright holder. It is the responsibility of the person downloading/uploading the material to

ensure no copyright is infringed.

4.5 Users must not use the internet in a way that denies access to others, for example by deliberate or reckless overloading of College systems.

4.6 Users should not import non-text files or unknown messages on to the College's system without having them scanned for viruses.

5. General Computer Usage

5.1 You are responsible for safeguarding your password(s) for College systems. For reasons of security, your individual password should not be printed, stored on-line or given to others. User password rights given to users should not give rise to an expectation of privacy.

5.2 Your ability to connect to other computer systems through the network does not imply a right to connect to those systems or to make use of those systems unless authorised to do so. You should not alter or copy a file belonging to another user without first obtaining permission from the creator of the file.

6. I.T. Services

6.1 The I.T. Services Department is there to assist you. If you require any information or help about the use or set up of your College computer you should contact I.T. Services via phone or E-mail.

7. Misuse of E-Mail or the Internet

7.1 The E-Mail and internet facilities provided by the College are provided on the understanding that users will use them in a responsible manner. However, misuse such as excessive private use of the E-Mail system during working hours or excessive private access to the Internet during working hours or knowingly downloading improper or obscene materials may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct, or result in a student's exclusion from their course and/or the College.

7.2 If the College considers that a user is abusing the Colleges policy it reserves the right to withdraw any of the facilities provided from any member of staff or student.

7.3 Use of the College's E-Mail systems, internet facilities including VPN connections will signify that a user has read and understood the above guidelines and has agreed to comply with these guidelines at all times.

8.0 PREVENT Agenda

In order to safeguard students utilising the IT facilities at the College and prevent individuals from accessing extremist materials via the College's network, we will ensure:

8.1 The organisation will retain the ability to log and retain records of all electronic communications (web browsing, e-mail traffic etc) by users on the College network.

8.2 Appropriate staff will be available to monitor any aspects of its telephony network, including mobile phones and any computing facilities made available to staff, students and visitors.

8.3 Only College approved software will be supported by the College and allowed to be used on the College network.

8.4 Any unauthorised software that breaches College policies and/or presents a risk to staff/student safety will be removed and appropriate action taken where necessary.

8.5 All unusual and/or suspicious events including breaches of security are to be reported immediately via the safeguarding team for further investigation.

Appendix 1

Data Protection Issues

Personal data is subject to the Data Protection Act 2018 (GDPR). Personal data includes any information about a living identifiable individual, including their name, address, phone number, e-mail address and any other information about the person. If you include such information in electronic communications or files, you are deemed to be processing personal data and must abide by the law. In particular, you must not collect such information without the individual knowing you propose to do this; you may not disclose or amend such information except in accordance with the purpose for which the information was collected; and you must ensure the information is accurate and up to date. In addition, the individual has the right to inspect what is held about him or her. The individual can demand correction of inaccurate information, can request blocking or erasure of damaging information, and can sue for damage caused by inaccurate information.

The law also imposes rules on the storage of personal data. Such data should only be kept for as long as it is needed for the purpose for which it was collected. If you maintain information systems containing personal data, you should ensure you abide by the data retention policy. This information should be held in such a way that it can be easily identified, reviewed and, when necessary, destroyed.

Finally, the law imposes strict rules on the transfer of personal data outside the European Economic Area (EEA). Transfer is not just the deliberate sending of information outside the EEA, but also allowing third parties from outside the EEA access to the personal data held in the UK.

Therefore, you should not:

- Use e-mails for any purpose that is not permitted under the College's notification under the Data Protection Act (GDPR) 2018;
- Use a false identity in any electronic communications you send out;
- Obtain, handle or disclose personal information without ensuring you are complying with the law;
- Allow third parties to read personal information by leaving your screen in view of such third parties;
- Create or forward advertisements, chain letters or unsolicited e-mails;
- Read other peoples' e-mails without their express permission or the permission of the Information Security Team;
- Pass on your password or ID to any third party;
- Invade someone's privacy by any means using electronic communication;
- Send any electronic communications containing personal information outside the EEA, or allow third parties outside the EEA to read your communications containing such information without checking with the College's Data Protection Officer.

You should:

- Be cautious about putting personal information in the body of the text, especially if it is of a sensitive or confidential nature. If you need to do so, follow the rules about encryption given above.

- Comply with a request from the Data Protection Officer, your manager or a member of the Executive to inspect your e-mail archives and/or to print out items relevant to a particular individual if that individual demands a copy of his/her file. This will only be requested when it is needed for a good reason, and the college procedures will be followed before obtaining the information.

- Be aware that you will be required to make available to the College all of your work related information systems (including electronic communications) when you leave the employment of the College;

Note that the recipients of your electronic communications including e-mails, the originators of e-mails you receive and the content of all e-mails sent or received may be the subject of scrutiny within current legislative provision.