IT Acceptable Use Policy 2022/2023

Change log

Version number	Changes description	Major changes? Y/N	Initiator	Rationale	Date of completion	New version number
V1	Creation	Y	Simon Ward	Requirement	2016	V1
V2	Amendments	N	Dave Hanlon	Review	07/2022	V2

CONTENTS

1. INTRODUCTION

1.1. The ability of individuals to use external e-mail and to access the Internet is encouraged by the College. It provides new opportunities to facilitate the gathering of information and communication with fellow employees, customers and other contacts. However, Internet and e-mail access opens up the College and individuals to new risks and liabilities. It is therefore essential that all users read these guidelines and make themselves aware of the potential liabilities involved in using e-mail and the Internet.

1.2. All internet / IT use is automatically monitored by systems that report any unacceptable use. Any breach of this policy by staff or students may result in disciplinary action and could potentially be classed as gross misconduct.

2. SCOPE

2.1. This policy applies to all persons who are authorised by Hopwood Hall College ("the College") to use its computer network, e-mail, internet and intranet through computers or other IT devices based at College premises, individuals homes or through computers at other sites (including private equipment) via the College's network.

2.2. This includes (but is not limited to) College employees, agency staff, volunteers, student teachers, learners, external partners and visitors (Users).

3. POLICY STATEMENT

3.1. This policy will not discriminate either directly or indirectly against any individual on grounds of sex, race or ethnicity, sexual orientation, religion or belief, age, disability, inclusion need, gender identity, socio-economic status or any other protected characteristic.

4. GENERAL POINTS

4.1. Use of all College IT (Information Technology) equipment, data storage, and all College related systems including the Internet is primarily for work-related purposes.

4.2. The College has the right to monitor any and all aspects of the IT systems that are made available to you and to monitor, and/or intercept communications made by users, including e-mail or Internet communications.

4.3. Computers, e-mail accounts or data stored on the College network 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 for any of the above, whether it is of a business or personal nature.

4.4. It is inappropriate in the use of e-mail and the Internet for users to intentionally access, download or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, defamatory or in any way discriminatory. You should be aware that such material may also be contained in jokes, images or videos sent by e-mail.

4.5. The College recognises that the Prevent agenda is fundamentally linked to the safety and safeguarding of our students and staff and it meets its responsibility of the Prevent

4.6. Duty under its safeguarding and child protection arrangements, through its Prevent Strategy and through this policy. The Prevent Strategy is written with reference to the Prevent Duty contained within Section 26 of the Counter Terrorism and Security Act 2015 which states that specified authorities including Further Education Colleges, in the exercise of their functions, must have "due regard to the need to prevent people from being drawn into terrorism". Where there is a disclosure or concern raised in relation to extremism or radicalisation, this policy will be utilised to gather information and evidence to support interventions or police / Channel enquires. This information will be shared with Channel where risks or vulnerabilities are identified.

4.7. Such misuse of electronic systems will be viewed as misconduct and will be investigated under the College's Disciplinary procedure. In certain circumstances, such misconduct may be treated by the College as gross misconduct. The College reserves the right to use the content of any employee or learner e-mail or an individual's browsing history in any disciplinary process. If you are concerned that you have accessed an inappropriate site unintentionally, please contact the IT Services department in person.

5. USE OF THE COLLEGE NETWORK (INCLUDING WIRELESS NETWORK AND BYOD)

5.1. This policy applies to all network users (staff, learners, visitors, etc.), including users of the wireless network (guest and staff) and equipment including laptops, mobile phones and tablets and other IT devices operating within the College.

5.2. If you have a Laptop, mobile phone, tablet, etc. you should be able to gain access to the wireless network operating across all College sites. College owned mobile equipment will be connected to the staff wireless and will be monitored by IT Services. All other mobile equipment can access the guest wireless and will be monitored by IT Services.

5.3. IT Services will continue to monitor, evaluate, develop and where applicable, incorporate new wireless network technology to the benefit of the College community.

5.4. Any breach of these guidelines will result in immediate action being taken. Action may include disconnection of any unapproved networking device and in the case of deliberate or repeated abuse may be treated as a disciplinary offence.

5.5. IT Services is responsible for authorising, managing and auditing connections to the College network for the security and integrity of the network. Records and logs are kept providing audit data for the purpose of tracking connectivity issues and possible misuse.

5.6. Users of the guest wireless network are responsible for their own computer equipment. Care should be taken when bringing in personal mobile devises for the use at college. The College cannot be held accountable for any loss, theft or damage to personal devices.

6. NETWOK ACCESS RESTRICTIONS AND GUIDANCE

6.1. In line with the Professional Guidance for Staff and Code of Conduct for learners, the College network whether accessed in College or remotely, should not be used inappropriately; in particular you should not use the network to:

6.1.1. send, receive or make available any material that might be considered offensive, obscene, indecent, discriminatory or extremist in nature.
6.1.2. send, receive or make available any material that might infringe copyright, e.g. audio and video files.
6.1.3. run file sharing software, e.g. Bit torrent, Rapid share, etc.
6.1.4. intercept or attempt to intercept other wireless transmissions for the purposes of eavesdropping.
6.1.5. access or run utilities or services which might negatively impact on the overall performance of the network or deny access to the network, e.g. RF jamming, Denial of Service (DoS).
6.1.6. harass, cause annoyance, nuisance or inconvenience to others.
6.1.7. access or attempt to access systems or resources to which you are not authorised (hacking).
6.1.8. provide services which may interfere with normal network operation.
6.1.9. provide access to others, e.g. allowing a third party to use your User Id and Password to access the network.

7. SECURITY AND MONITORING

7.1. IT Services are responsible for maintaining the availability of the College wired and wireless networks. In order to better manage and monitor the networks, and to identify rogue devices and possible misuse of the network, IT Services do make periodic sweeps of the College network and in strategic locations, make use of passive monitoring devices and intrusion detection software.

7.2. If IT Services have reasonable grounds for believing that any equipment may be the cause of unacceptable degradation of the performance of the network detrimental to other Users, then the User must co-operate with the disconnection of the equipment from the network pending resolution of the problem.

7.3. To mitigate the College's exposure to external threat, users' wireless devices must:
7.3.1. run an anti-virus software and maintain any virus definition updates.
7.3.2. ensure that their operating system is fully patched and running the latest service packs.
7.3.3. not run in ad-hoc mode, i.e. peer-to-peer mode.

7.4. If users of the wireless network are in any doubt as to how to maintain their particular device, assistance can be gained in the first instance through the iLearn or Technology Shop.

7.5. IT Services reserve the right to inspect any wireless device to ensure the requirements of the IT Acceptable Use Policy are being met. Wireless devices should also be made available for inspection in the event of a breach of this Policy.

7.6. All data stored on College systems is the property of the College. College data is only permitted to be stored on the college network or on the College's subscription to the Office 365 service. It is not acceptable for staff to make local copies or take data off-site unless this is on an encrypted college owned laptop.

7.7. Where sensitive data is to be stored, encryption technology and a password must be enforced. If you require any clarification regarding this, please contact IT Services. Further information can be found in the College's Data Protection and Information Governance Policies.

8. USE OF COLLEGE TELEPHONES

8.1. The College appreciates that there may be occasions where individuals need to use the telephone during working hours. Reasonable use of the College telephone system for private use is permitted where this is necessary for emergencies or on an ad-hoc basis, but this should not interfere with your work.

8.2. Payment should be made for calls users feel may be excessive. These should be recorded with the Finance Department. The cost of your calls will be calculated and payment should be made to the Finance team.

8.3. If you feel you have a requirement to use the telephone for what could be interpreted as more than reasonable, please discuss this with your Line Manager or the Human Resources Department.

8.4. Telephone calls are not routinely monitored. However, the College reserves the right to monitor the College telephone bill and investigate continuous recurring numbers or longer calls.

8.5. As per the Professional Guidelines for Staff, personal mobiles phones should not be used during working hours, unless this is during agreed breaks or an emergency situation.

8.6. Personal contact details, such as mobile numbers, should not be given to students.

8.7. Excessive private use of the telephone for personal use may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

9. USE OF COLLEGE OWNED MOBILE PHONES

9.1. Any member of staff allocated a college owned mobile phone is responsible for adhering to the following code of conduct:

9.1.1. Ensuring the adequate physical security of the device.
9.1.2. Maintaining the software configuration of the device – both the operating system and the applications installed.
9.1.3. Preventing the storage of sensitive data on the device.
9.1.4. Ensuring the device's security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes.
9.1.5. Reporting a damaged, lost or stolen device immediately to IT Services.
9.1.6. Ensuring the phone's Wi-Fi is always on to reduce costly charges incurred when data allowance is exceeded.

9.1.7. Any additional costs arising from the data allowance being exceeded may be recovered from the relevant department.

9.1.8. Not to use the phone whilst driving or in an area where it may cause a risk to health and safety e.g. Building Site.

10. USE OF EMAIL

10.1. 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.

10.2. E-mail should not be used as a substitute for face-to-face communication. Abusive emails can be a source of stress and damage work relationships. Hasty messages, sent without proper consideration, can cause unnecessary misunderstandings.

10.3. Users should not make derogatory remarks in e-mails about employees, learners, competitors or any other person. Any written derogatory remark may constitute libel. Care should always be taken to ensure that email content can never be construed as bullying, harassment or discriminatory.

10.4. Users should not create e-mail congestion by sending trivial messages or unnecessarily copying e-mails.

10.5. Hard copies of e-mails which staff may need to retain for record keeping purposes must conform to the College's Data Protection and Storage of Information procedures. For more information, please refer to the Data Protection Policy.

10.6. Use of College e-mail account for personal use should be restricted and should not interfere with your college work. Frequent, excessive and time consuming personal email correspondence during the working day is likely to be found to be unreasonable. When using College emails for personal use, all content must comply with the restrictions set out in the Professional Guidelines for Staff and code of conduct for learners. Excessive private use of the e-mail system during working hours may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. The College also reserves the right to withdraw individuals Email privileges in such cases.

10.7. The use of College email accounts for personal use should be restricted as above and should never be used for social networking sites, on-line banking, on-line auctions sites etc.

10.8. By sending e-mails on the College's system, you are consenting to the processing of any personal data contained in that e-mail and are explicitly consenting to the processing of any sensitive personal data contained in that e-mail. If you do not wish the College to process such data you should communicate it by other means.

11. EMAIL RESTRICTIONS

11.1. The College will not accept the use of e-mail in the following circumstances:

11.1.1. Any engagement in activities that are illegal;
11.1.2. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses etc.);
11.1.3. Active engagement in procuring or transmitting material that is in violation of harassment or workplace laws and/or regulations;
11.1.4. The authoring or transmission of any message that could be considered to be obscene, abusive, sexist, racist or defamatory or could constitute bullying, harassment, discrimination or extremist in nature;
11.1.5. On-line gambling;
11.1.6. Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail Spam);
11.1.7. Access to the e-mail system using another user's password;
11.1.8. Unauthorised distribution of copyright information and / or any software available to the user;
11.1.9. The unauthorised transmission or distribution of confidential information about other staff, Corporation members, the College or its students/customers or suppliers;
11.1.10. Excessive personal use for social invitations or personal messages;
11.1.11. The use of College email address for commercial or business purposes;
11.1.12. The transmission of jokes, cartoons, banter or chain letters whether or not they fall within the scope of bullying, harassment and/or discrimination, as detailed in the College's Equality, Diversity and Inclusion Policy and e-safety guidelines;
11.1.13. The unauthorised transmission of offers or contracts to third parties, contractors or suppliers in respect of goods, services or employment;
11.1.14. The authoring or transmission, distribution or forwarding of materials from third parties which may be offensive or contain racist, discriminatory or pornographic images or statements; or that promotes a particular agenda E.g. political, religious or extremist; contrary to the Single Equality Scheme, Prevent Strategy, e-Safety Policy and the Safeguarding and Child Protection Policy.

11.2. The above list is not exhaustive, but attempts to provide a framework for activities that fall into the category of unacceptable use. Contravention of the above restrictions may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

11.3. Users who feel that they have cause for complaint as a result of e-mail communications should raise the matter initially with their line manager and/or through the College Complaints procedure. If necessary, the complaint can then be raised through the College grievance procedure.

12. USE OF THE INTERNET

12.1. Reasonable private use of the Internet is permitted for users, but this should be kept to a minimum and should not interfere with your work. Frequent or time consuming use of the internet for personal use during the working day is likely to be found to be unreasonable and may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. The College also reserves the right to withdraw individual's internet privileges in such cases.

12.2. The sites accessed by you must comply with the restrictions set out in these guidelines. Accessing inappropriate sites with intent may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct. The College also reserves the right to withdraw individual's internet privileges in such cases.

12.3. **Internet Restrictions**: The College will not accept the use of the internet for:

12.3.1. On-line gambling;
12.3.2. Accessing pornography;
12.3.3. Accessing racist, discriminatory or extremist materials;
12.3.4. Use in connection with employment, engagement or business outside the College;
12.3.5. Unauthorised downloading or distribution of copyright information and/or any software available to the user;
12.3.6. The posting of confidential information about staff, Corporation members, the college or its students/customers or suppliers.
12.3.7. Attempting to circumvent safeguarding systems, which are in place to restrict access.

13. ACCESS TO INAPPROPRIATE / ILLEGAL CONTENT

13.1. In line with the College's Safeguarding and Child Protection Policy, the Professional Guidelines for Staff and Code of Conduct for learners; there are no circumstances that will justify adults possessing indecent images of children. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will be reported to the Disclosure and Barring Service (DBS), the Local Authority Designated officer (LADO) and may lead to criminal investigation and the individual being barred from working with students, if proven.

13.2. Users should not use either their own or college equipment (including mobile phones) or network services to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children. This will be reported to the Disclosure and Barring Service (DBS) and may lead to criminal investigation and the individual being barred from working with students, if proven.

13.3. Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) will be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution. The College's Allegation Management Policy should be used and the Senior Safeguarding Officer should be contacted.

13.4. Accessing or possessing inappropriate images will be classed as gross misconduct, and following investigation under the College's Disciplinary policy, is likely to result in dismissal or exclusion.

14. REPORTING ACCESS TO INAPPROPRIATE / ILLEGAL CONTENT

14.1. The College takes seriously its responsibility to ensure the safety and wellbeing of its staff, learners and users of IT equipment as well as its legal and moral duty to safeguard against the use and distribution of illegal or inappropriate messages, pictures or content. Whilst the College has in place adequate monitoring and filtering systems, there may be occasions when these systems are by-passed.

14.2. If staff come across any inappropriate or illegal messages, pictures or content, whether on College websites, emails or external sites, this should be reported to the Head of IT Services so the appropriate procedures can be followed.

15. SOCIAL NETWORKING SITES

15.1. The internet is provided primarily for business / studying use. The College recognises that many individuals use the internet for personal purposes and may participate in social networking on websites such as Facebook, Twitter, etc.

15.2. The College restricts access to social networking sites. Access is limited to the hours of 12:00-14:00 and should only be used during agreed breaks. All other internet access for personal use must be done in accordance within reasonable usage rules laid out in this document. The College does however reserve the right to restrict access to these websites at any time and without notice.

15.3. In line with the Professional Guidelines for Staff and the Safeguarding Policy, staff should ensure that if a social networking site is used, details are not shared with students and privacy settings are set at maximum. Staff should not add students or their families as friends on their own social networking sites. Any relationships at work should be disclosed as per the procedure detailed in the Professional Guidelines for Staff.

15.4. Security and identity theft: Users should be aware that social networking websites are a public forum, particularly if the employee is part of a 'network'. Users should not assume that their entries on any website will remain private. Users should never send abusive or defamatory messages.

15.5. Users must also be security conscious and should take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites allow people to post detailed personal information such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords. In addition, users should:

15.6. ensure that no information is made available that could provide a person with unauthorised access to the College and/or any confidential information; and

15.7. Refrain from recording any confidential information regarding the College on any social networking website.

15.8. All users of the IT facilities at the College must not use any devices, personal or College owned, to record and upload or share audio or video recordings of any other students or staff members without their knowledge and agreement. This is expressly forbidden. If there are found to be audio or videos shared online without

agreement as part of any investigation, this may lead to disciplinary action and may lead to intervention with the relevant authorities.

16. PERSONAL CONDUCT

16.1. The College respects an individuals' right to a private life. However, the College must also, at all times ensure that confidentiality and its reputation, its staff, learners and stakeholders are protected. It therefore requires individuals in their use of ICT to:

16.2. ensure that they do not conduct themselves in a way that is detrimental to themselves, their colleagues, students or the College; and

16.2.1. Take care not to allow their interaction to damage working relationships between members of staff/students and clients of the College; and

16.2.2. ensure that the boundaries of proper and professional relationships are maintained;

16.2.3. Ensure that any interaction causes no detriment to the reputation of the College or its employees, students or clients;

16.2.4. ensure that personal social networking sites are set at private and learners are never listed as approved contacts;

16.2.5. Never use or access social networking sites of learners;

16.2.6. Staff should be mindful that they should apply Professional Guidelines to them within and outside of the workplace including use of social media.

16.3. Any breach of the above code of conduct may lead to disciplinary action and may in certain circumstances be treated by the College as gross misconduct.

17. COLLEGE TEXT MESSAGING

17.1. The ability to use text messaging provides new opportunities for the College as it facilitates the spread of information to potential students, parents, current students and colleagues. However, it also presents new risks and liabilities and it is therefore essential that users read these guidelines and make themselves aware of the potential liabilities involved in using text messaging.

17.2. Failure to comply with the rules and conditions set out below may lead to disciplinary action, or dependent upon the seriousness of the breach, possible criminal action.

17.3. Text messaging restrictions and guidance:

17.3.1. Text messaging should only be used for work related purposes.

17.3.2. The college reserves the right to monitor any and all aspects of its telephone and computer system and may intercept, and/or record any communications made.

17.3.3. The text messaging service (ConnectTxt) provided, is the property of the College and is designed to assist work performance.

17.3.4. Users should not transmit material which might reasonably be considered to be obscene or otherwise inappropriate and users must be aware that such material may also be contained in jokes.

17.3.5. Text messages should be drafted with care. Due to the informal nature of text messaging, it is easy to forget that it is a potentially permanent form of

written communication that can be saved by the recipient. You must therefore treat text messages as you would any other business communication.

17.3.6. The College's text messaging system is not to be used for transmitting unlawful, or what the College considers, in its absolute discretion, to be inappropriate, offensive, defamatory, obscene or pornographic material. This includes but is not limited to messages that contain racist, sexist, discriminatory or extremist material.

17.3.7. All information leaving the college in text form must reflect the standards and policies of the college and breach of this rule may be treated as a disciplinary matter.

17.3.8. No text messaging service is totally secure. Consequently, information of a confidential or personal nature should not be sent unless expressly required by the intended recipient who must be made aware of the potential risk before the text is sent.

17.3.9. Copies of text messages may have to be disclosed in litigation. Before you send a message, think carefully about its content and ask yourself how you would feel if you received that message or know that it may be disclosed in court. For more information, refer to the Professional Guidelines for Staff.

17.3.10. Furthermore, a text message may constitute a contract, so ensure that your language does not indicate a commitment that you cannot keep or are not authorised to make.

18. COPYRIGHT AND DOWNLOADING

18.1. Copyright applies to all text, pictures, video and sound, including those sent by e-mail or on the Internet. Files containing authorised copyright protected material may be downloaded, but not 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.

18.2. Posting copyright material to any social media site or website related to the college, without the express permission or licence to do so from the copyright owner may be treated as a disciplinary matter.

18.3. Unauthorised downloading of copyrighted software must never be carried out.

19. GENERAL IT EQUIPMENT USAGE

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

19.2. 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.

19.3. Users must not load any additional software onto the IT systems without the prior approval of IT Services. It is the responsibility of IT Services to ensure that the appropriate licences are obtained for all software. All attached terms and conditions of use must be adhered to.

19.4. Any damage or loss due to negligence to IT Equipment which is allocated to an individual under the IT Equipment allocation policy, the full cost of repair or replacement may be charged back to the individual via the department Head. This includes but not restricted to dropping of equipment or leaving in an unsecure location e.g. Car etc. The department Head takes ownership and accountability of all IT resources utilised in their department.

19.5. Willful damage or interference adversely affecting the performance of the College's IT facilities is strictly forbidden. This includes but is not restricted to the following actions:

19.5.1. Attempts to interfere with equipment and cabling.
19.5.2. Introduction of Viruses.
19.5.3. Use of consumables such as printer paper for other than the intended use.

19.6. All users of the College's IT facilities must comply with the relevant parts of UK law, including:

19.6.1. The General Data Protection Regulation 2018
19.6.2. Copyright, Designs and Patents Act 1988
19.6.3. The Computer Misuse Act 1990

20. IMPLEMENTATION

20.1. The Head of IT is responsible for the management of the e-mail and Internet system. The IT Services department are available for advice on all aspects of the IT Acceptable Use Policy.

20.2. Induction training is available to familiarise users with the e-mail and Internet system and its uses. Online training of Microsoft related products is available via the Hub.

20.3. Users who feel they have cause for a complaint as a result of e-mail communication should raise the matter initially with their immediate line manager. If necessary, the complaint can then be raised through the appropriate College procedures. If the complaint is about your line manager, direct the complaint to either HR or the Head of IT Services.

20.4. This policy will be distributed to staff via the College's Netconsent System and a copy will be accessible via the Hub. The policy overview will be available to learners via induction and through ItsLearning.

21. APPENDICES AND RELATED DOCUMENTS

21.1. This policy should be read alongside the 'Professional Guidelines for Staff' and 'Code of conduct' for learners which can be found in the Human Resources library on the staff intranet or on ItsLearning.

21.2. This ICT Acceptable Use Policy links to a number of other key policies and documents within the College, namely:

21.2.1. Professional Guidelines for Staff
21.2.2. Code of Conduct for Learners
21.2.3. Safeguarding and Child Protection Policy
21.2.4. Equality, Diversity and Inclusion Policy
21.2.5. Bullying and Harassment Policy
21.2.6. E-Safety Guidelines
21.2.7. Password Policy
21.2.8. Equipment Allocation Policy
21.2.9. Prevent Strategy
21.2.10. Disciplinary Policies
21.2.11. Allegation Management Policy
21.2.12. Freedom of Information Policy
21.2.13. Data Protection Policy
21.2.14. Whistle Blowing Policy

22. DOCUMENT REVIEW INFORMATION

22.1. Policy Date: July 2022
22.2. Policy Author: Dave Hanlon
22.3. Date of SLT Sign Off: July 2022
22.4. Equality Impact Assessment Completed? Yes
22.5. Equality Impact Assessment Date: Sep 2022
22.6. Next Policy Review Date: July 2024