IT Acceptable and Safe use policy

1. Policy Statement

1.1 Use of IT systems is subject to the legislation relevant to the use and monitoring of electronic communications predominantly Regulation of Investigatory Powers Act 2000; the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000; GDPR and the Data Protection Act 2018; the Copyright, Designs and Patents Act 1988 and subsequent regulations, Safeguarding including the Terrorism Act (2006), and the Computer Misuse Act 1990 as well as other relevant college policies.

1.2 In order to comply with legislation the College will monitor any IT related activity. The College cannot guarantee absolute privacy whilst using IT systems, regardless of whether this is for business or personal use.

2. Scope

2.1 The following policy applies to all employees, temporary staff, students, governors, volunteers and visitors (hereafter referred to as users) of the College who have access to and are using the IT systems owned, leased or hired by the College both on the premises and remotely or when using any device with College credentials/authentication to access college IT systems.

2.2 Our approach is to implement appropriate safeguards within the College which supports all users to identify and manage risks independently and with confidence. We believe we can achieve our aims through a combination of security measures, training, guidance and the implementation of our policies. In accordance with our duty to safeguard users and the PREVENT agenda, we will do all that we can to make our users aware of the precautions they should take to be safe online e and to satisfy our wider duty of care. We aim to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent.

3. Roles and responsibilities

3.1 There are clear lines of responsibility for IT acceptable usage, PREVENT and online safety within the College. This responsibility is shared across the following groups/roles:

- Director of IT (Infrastructure and Technical Services) or depute with the Assistant Principal Teaching & Learning
- Director of Admissions and Marketing
- Prevent and Online Safety group – has representation from SLT, Safeguarding, IT & Estates
- Data protection & Security – has representation from SLT, Governance, HR, IT & MIS

It is the their responsibility to collectively review and update this Policy with the Director of IT (Infrastructure and Technical Services) or depute leading, deliver relevant staff development and training, report any developments and liaise with the Senior Leadership team and external agencies as needed to promote IT acceptable usage and online safety within the College community.

3.2 All users must act safely and responsibly at all times when using the College IT systems or credentials/authentication. Students are responsible for attending IT acceptable usage, PREVENT and online safety lessons as part of the aspire programme and they are expected to know and act in line with other relevant college policies such as those detailed in section 20. All relevant policies are available to access and download from the College's VLE (Moodle).

3.3 Students must electronically sign a reference to this policy which is stored within CEDAR (Student Record Portal)

4. Acceptable use

4.1 Any attempts to corrupt, disable, defeat, destroy or circumvent any of the College's IT infrastructure systems or credentials/authentication will be treated as a potential act of gross misconduct

4.2 Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to any illegal activity. Please refer to examples listed in **Appendix A – Examples of illegal activity**

4.3 Users shall not undertake activities that are classed as unacceptable to the college. Please refer to examples listed in **Appendix B – Examples of unacceptable activity**

4.4 The College recognises that it may sometimes be necessary for users to carry out personal tasks using the College's IT facilities (i.e. send/receive personal emails, make/receive personal phone calls and carry out private research on the internet). Credit card details (personal or college credit card) must not be typed into the text of an email or attachment. Users should not allow this to impinge on normal working/study hours. Personal use may in certain circumstances be treated as misconduct.

4.5 All users must not make remarks in electronic communications about other users or stakeholders that could be considered obscene, abusive, sexist, racist, extreme, radical and/or defamatory or that contravene the anti-bullying and harassment policies for staff and students. Any written derogatory remark may constitute libel.

4.6 Users utilising or administering the College's IT systems or credentials/authentication must not try and prove any suspected or perceived security weaknesses.

4.7 All actual and suspected security incidents (deliberate or accidental) must are to be reported to the Director of IT (Infrastructure and Technical Services) or deputy immediately who will determine the nature or need of any escalation and consideration will be given to ICO deadlines for reporting data breaches if required

4.8 All users must ensure they use only college approved applications, software and systems (including cloud hosted/websites that require authentication using college accounts or email) that are logged on the information asset register and/or IT software inventory so we meet GDPR and Cyber security requirements.

4.9 All users are responsible for safeguarding their password for the College IT systems. For reasons of security, individual passwords should not be printed, stored online or given to others.

4.10 All users are required to manage their individual or shared file storage e.g. OneDrive, Teams, Shared Drives, H Drive appropriately and delete any items that are no longer required. Files containing personal data should be structured in a way that they can easily be identified and removed when processing is no longer necessary or in line with the relevant college privacy notices.

5. Bring Your Own Device (BYOD)

5.1 Bring Your Own Device (BYOD) means accessing College systems and information through personally owned devices; such as tablets, smartphones, smart watches, laptops and PCs. You must ensure BYOD devices meet the following before connecting to the HNC BYOD/Guest networks onsite and/or accessing College systems and data from anywhere with an internet connection:

- Staff are required to register personally owned devices via a Microsoft Form before use
- Devices must be running the latest operating system, application updates, and security updates:
  - Run only software/applications/browsers that are used and up to date with the latest updates
  - Remove or disable all the software that you do not use on your device and remove any unsupported software on your device, unsigned applications must not be installed

- Run an operating system that is supported by the manufacturer and still receives security updates
- Windows, Mac OS, and Linux devices must use a software firewall which needs to be configured and enabled at all times and be running up to date Antivirus software
- Devices must be free of any malware and have anti malware software installed which:
  - Has daily updates enabled and scans files upon access
  - Is configured to scan & warn about accessing malicious websites upon access
- Devices must not be rooted/jailbroken and all apps must be installed from official sources, for example, Apple and Android apps must be installed from Apple's App Store & Google Play Store
- Devices must be secured with a strong password or 6 digit passcode (also see password section) with an auto-lock (device/screen locks automatically after an idle time period)
- Passwords and PINs must be changed immediately if they are known to be or suspected of being compromised. Do not allow cached/remembered passwords to protect college systems
- Access to college systems should be via the relevant staff or student portal page using supported and up-to-date browser (Microsoft Edge or Google Chrome) from the official apps store or download page for the device in question. If using an app you must use the approved apps below for accessing Organisational data:
  - Microsoft Corporation – Microsoft 365 (Office) Apps, Microsoft Teams App, OneDrive or Outlook app
  - Microsoft Office applications downloaded via the colleges Office 365 on the relevant portal page
  - Moodle Pty Ltd – Moodle app
- Users may use the systems listed above to view college information via their mobile devices, including information about students. Staff must not store the information on their devices, or on cloud servers linked to their mobile devices. In some cases, it may be necessary for staff to download college information to their mobile devices to view it (for example, to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it. Where personal or sensitive data is used in this way devices or files MUST be encrypted.
- The use of Microsoft Remote Apps is available on request to staff only via a Cedar ticket to IT Support. This give access to onsite applications, secure network file storage and secure shared areas.
- Users shall ensure that unauthorised persons (friends, family, associates, etc.) do not gain access to mobile systems, devices or information in their charge.
- If using Public Wi-Fi/free Wi-Fi avoid using College systems or online accounts which hold sensitive information and make sure the URL starts with HTTPS not HTTP.
- Turn off Wi-Fi on devices when not being used in a public place to avoid automatic connection to open networks.

6. Communications

6.1 For all users any information regarding specific details of College business must be communicated using the College email addresses provided for this purpose. This ensures all email traffic meets the requirements of this policy. College emails should be kept secure by not setting forwarding rules to other email accounts e.g. personal email accounts

6.2 All digital communications must be professional, in line with College policies, and lawful at all times. Using personal e-mail/social networking/messaging to carry out digital communications is not allowed.

6.3 For staff, use of the standard college email signature is required as this contains a legal disclaimer. A guide on how to apply this signature is available on Moodle

7. Copyright

7.1 Copyright applies to all text, pictures, video and sound (including music streaming services), including those sent by email or via the internet. Files containing such copyright protected material should not be copied, downloaded, forwarded, transmitted or broadcasted to third parties without prior permission of the author of the material or an acknowledgement of the original source of the material, as appropriate.

7.2 All users should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

7.3 Copyrighted software must never be downloaded and installed on any College device unless approved and used within the relevant software licences obtained, all software/systems/applications must be used in compliance with any terms of use/software licence terms.

8. Data protection

8.1 No College data should be shared electronically with any third party without the prior permission of the Data Protection Officer (DPO). If agreement is in place, the information must be encrypted. All users must ensure the safety of personal data by not displaying, holding or transferring data in an insecure manner

8.2 All devices used to access College systems and data e.g. mobile devices such as a laptop or phone must be password protected. No personal data should be stored locally e.g. downloaded from teams/cedar.

8.3 Removable Media & Encryption:

- Users should not use unofficial media, such as USB sticks or removable media devices. If the use of these are critical, then the advice of the DPO should be sought and the devices should be encrypted securely. Devices should always be stored and transported safely and recorded on the Information Asset Register by the DPO.
- No sensitive information or personal information should be stored on USB sticks or removable media devices. If this has been agreed by the DPO and is identified on the Information Asset Register then the files sent should be encrypted using the College procedure available on Moodle.
- No sensitive information or personal information should be sent via email to internal or external contacts. If this has been agreed by the DPO and is identified on the Information Asset Register then the files sent should be encrypted before sending using the College procedure available on Moodle.
- College owned removable media must be formatted or destroyed by the IT Support team only.
- USB sticks and removable media devices are automatically scanned for viruses/malware using the College's Endpoint protection software when used in a College device.
- Report any incidents to the DPO including the loss or compromise of a device so appropriate action can be taken e.g. if college device it will be remotely disabled/denied access to the network.

8.4 Please refer to the College website for full details of our Data Protection Policies: https://www.huddnewcoll.ac.uk/about-us/our-policies

9. Digital and video images (including video calls/conferencing)

9.1 The use of images, captures or videos should be encouraged where there is no breach of copyright, data protection or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to users. When using digital and video images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images.

9.2 Images, captures or videos of students should not be taken using staff personal devices. College owned devices should be used at all times. These must be securely stored and removed when no longer necessary and in line with the college privacy notices for GDPR

9.3 The College has subscribed to various video capture platforms which should be used only as a tool for staff to capture, reflect on, analyse and share their teaching/organisational practice or for their professional development.

9.4 The College may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies. The College has various video calling/conferencing platforms recommended which can be used as a learning and working tool, however the guidance below should be followed:

- Only setup video calls/conferences on systems recommended by the college and where students are identified and secured by their College login details, do no ask students to join conferences where they have to use their private email or contact details
- As the host you should record your video call/meeting and you should let participants know that you are about to do this before you start – it will allow you to share the recording with anyone who missed the live event and additionally acts a safeguarding check
- As the host use the video facilities to allow your students to see you if you would like to (although you might just want to check what else they can see behind/around you first)
- Staff decide if Students should have their camera/microphones on for their online learning sessions
- All users should check surroundings e.g. what can be seen behind/around you before turning cameras on and should be dressed appropriately
- When 1 to 1 video calls with students are deemed necessary, these should be recorded for safeguarding purposes to protect all users
- Encourage students to use the text chat function to ask/answer questions. Students may have a microphone, but they may not. It can also become quite chaotic with multiple voice participants!
- Be respectful of other users in the language that you use and your behaviour on the video call/conference
- If users have any concerns that arise from using video calls/conferences please email safeguarding@huddnewcoll.ac.uk in a remote working environment or log in the normal way via Progress Tutor for Students and via a Cedar safeguarding log for Staff

10. Filtering

10.1 The College forbids all users to use College's IT systems or credentials/authentication in order to access, download and/or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, extreme, radical and/or defamatory or contravenes the anti-bullying and harassment policies for staff and students.

10.2 The Terrorism Act (2006) outlaws web posting of material that encourages or endorses terrorist acts, even terrorist acts carried out in the past. Sections of the Terrorism Act also create a risk of prosecution for those who transmit material of this nature, including transmitting this material electronically. Visits to websites related to jihadism and downloading of material issued by jihadist groups (even from open-access sites) may be subject to monitoring by the Police.

10.3 The College uses a powerful web filter in order to prevent access to inappropriate websites including accessing radical and/or extremist websites and materials, this forms part of the College's obligations in line with the PREVENT Duty. All users should be aware that all access to the internet is recorded and logged by this web filter. Alerts are in place to monitor breaches of this policy. Due to the nature of the filter, some sites/site categories may be blocked which are appropriate to College business or teaching, learning

and assessment. In these cases, the member of staff should request these sites to be unblocked through a CEDAR ticket to IT Support.

10.4 Web filtering will be reviewed periodically to make sure its meets with the PREVENT Duty/Online Safety and other Government advice provided by the Department for Education or National Centre for Cyber Security. Access to online gambling sites is prohibited in accordance with this policy.

10.5 Web filtering on IT systems owned, leased or hired by the College both on the premises and remotely are subject to HTTPS inspection (standard security settings of third party sites).

11. Monitoring

11.1 The College has the right to monitor any aspects of its IT systems that are made available to any user and may also monitor, intercept and/or record any communications made, including telephones, email, digital or internet communications. The College will ensure compliance in line with the Regulation of Investigatory Powers Act (RIPA) 2000, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

11.2 IT Systems e.g. Computers, electronic devices, storage, credentials/authentication and accounts are the property of the College and are designed to assist in the performance of your work or study. Users should be aware that any usage of the College's IT systems or credentials/authentication remain the property of the College; this may be stored data, emails, images etc. You should, therefore have no expectation of privacy in any of your stored work.

11.3 All users should have no expectation of privacy in any communication sent or received e.g. email, teams chat messages, whether it is of a business or personal nature. College communication platforms are primarily provided for your use in performing your College duties and personal use should be avoided where possible. The content of communication e.g. email, teams chat messages and data storage will be monitored and subject to spot checking to ensure compliance.

11.4 For business continuity purposes, the College may need to check the emails of employees who are absent. The IT Services team will facilitate this with the relevant line manager or SLT lead when a request is logged via the Cedar helpdesk

11.5 Copies of emails/communications and/or data stored may need to be publicly available under the Freedom of Information Act 2000, and/or as part of a criminal investigation.

12. Online Safety

12.1 Staff and Governors are responsible for ensuring the safety of students and must report any concerns immediately to the Progress Tutor team. When informed about an online safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

12.2 Staff and Governors must electronically sign this policy and this will be stored by the College. Staff are responsible for attending staff training on IT acceptable usage, PREVENT and online safety.

12.3 Visitors would be expected to report any concerns to Reception, who will inform the Director of IT (Infrastructure and Technical Services) or depute. Visitors electronically sign into the college on entry and have to read, acknowledge and electronically sign, agreeing to our expectations.

12.4 Students know what to do if they have online safety concerns and who to talk to. In most cases, this will be their Progress Tutor. Where any report of an online safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, a member of the safeguarding team may be asked to intervene with appropriate additional support from external agencies.

13. Password Management

13.1 All users of the College systems must adhere to the password policies defined below in order to protect security, data integrity and computer systems

13.2 Password Guidance:

- A password that is difficult to guess will be unique and not be made up of common or predictable words such as "password" or "admin", or include predictable number sequences such as "12345"
- Put random words together or use a random password generator
- Use numbers, symbols, upper-case letters, lower-case letters in a random order
- Try to use a different password for each online account, if you can remember them without prompt
- Your college account and personal email account must have separate strong passwords
- Avoid passwords that could be easily picked up from information in your online presence and personal information e.g. sports teams followed, pets name, family names etc.
- Don’t insecurely store passwords as these can be stolen, such as ones written on sticky notes etc.
- Don't use common words or reverse spelling of words in any part of your password.
- Don't use names of people or places as part of your password.
- Don't use part of your login name in your password.
- Don’t use personal information such as names of family members, addresses or phone numbers.
- Never reveal a password on questionnaires or security forms.
- Use multi-factor authentication (MFA) or Two-factor authentication (2FA) where provided for all accounts. This helps stop hackers from getting into your accounts by asking for more information to prove your identity, such as a code that gets sent to your phone or approval via an authenticator app
- A minimum password length of 8 characters and no maximum length applies
- Saving your password in your browser means letting your web browser (such as Chrome, Safari or Edge) remember your password for you
- If you suspect someone has your password or your account has been compromised, you must inform the IT Services team immediately by phoning 4663 or 4661 and they will secure your account and advise what steps need to be taken

13.3 Password/Device Protection of accounts/data:

- Accounts will reach lockout threshold after 10 failed login attempts
- Account lockout duration will be 15 minutes, after this time it will unlock automatically
- The last 12 passwords you use on the system cannot be reused
- Never share your password
- Devices should not be unattended with the user logged on. Users should be in the habit of not leaving their computers unlocked. They can use the short sequence Windows key plus L or press the CTRL-ALT-DEL keys and select "Lock Computer".

13.4 Resetting a forgotten password:

- In person; bring your College membership badge to the IT Services Office (Room 524)
- By email/phone; quote your username, full name and department. You will be asked to confirm security questions
- When you receive your new password, you must change it as soon as possible as this password will be single use only

14. Privacy & Website (Cookies)

14.1 A Cookie is a text file placed on your computer. It enables websites to identify you as you view the different pages and applications on our website.

14.2 This site uses some unobtrusive cookies to store information on your computer. Some cookies on this site are essential, and the site won't work as expected without them.

14.3 These cookies are set when you submit a form, login or interact with the site by doing something that goes beyond clicking on simple links.

14.4 We also use some non-essential cookies to anonymously track visitors or enhance your experience of the site. If you're not happy with this, we won't set these cookies but some nice features of the site may be unavailable. To control third party cookies, you can also adjust your browser settings.

14.5 We will always hold your data securely and not provide your information to any third parties. More details are available in our Data Protection policy, which is available on our website.

14.6 We work closely with our website provider to ensure there are processes for identifying security vulnerabilities on the college website and that these are resolved within a timely manner

14.7 We're committed to making our website as accessible as possible to all audiences (including those with visual, hearing, cognitive or motor impairments) to meet its requirements under the Disability Discrimination Act, more information is in our accessibility statement on the college website

15. Retention of accounts/data

15.1 Staff and governor emails will be stored in Office 365 for 36 months. Automatic deletion at this point will take place regardless if the user has utilised the archive facility or saved the email to folder within the mailbox.

15.2 Staff and governors whose contracts (or terms of appointment) have ceased; emails and Home drive files will be kept for 12 months before absolute deletion.

15.3 Staff and governors whose contracts (or terms of appointment) have ceased; OneDrive files will be kept for 30 days before absolute deletion (this is part of the Microsoft agreement)

15.4 Students who have left or completed education at Huddersfield New College; Home drive files will be kept for 12 months before absolute deletion (this satisfies vocational requirements regarding the retrieval of work).

15.5 Students who have left or completed education at Huddersfield New College; emails and OneDrive will be kept for 30 days before absolute deletion (this is part of the Microsoft agreement).

15.6 When users leave the College their access rights to all systems and data will be removed.

15.7 When staff change jobs within the College their access rights will be reviewed and changed as necessary. A periodic check will be made for redundant user identities and these will be removed.

16. Security

16.1 The College will take all necessary and reasonable steps to ensure the College network is safe and secure. Every effort will be made to keep security software/settings up to date, we run regular PEN testing and vulnerability assessments to identify any weaknesses and make improvements to our systems. The College has appropriate security measures in place; these include the use of enhanced email protection, firewall protection, end-point protection (including anti-virus software). This is to prevent accidental or malicious access of college systems and information.

16.2 Staff undertake mandatory certificated GDPR and Cyber Security awareness training annually, progress and compliance is checked

16.3 Student training for Cybersecurity (using NCSC materials) is mandatory and progress is tracked via the fundamentals programme

16.4 Staff and Governors will participate in simulated phishing tests (email phishing tests), these are designed to evaluate response in spotting a false phishing emails using campaign templates with varying levels of difficulty levels to detect. This helps us to determine the area of cyber security where we needed to focus further training and development. Where staff and governors fail/fall for these tests we have different levels of actions taken:

- One failure in 12 month period – email from Director of IT to user cc Line Manager, log on College IP, follow up training
- Two failures in 12 month period – email from Director of IT to user cc Line Manager, log on College IP, follow up training, separate email to line manager to request for an informal meeting be held with the user to discuss the failures, ensuring the user is aware a 3rd failure in a 12 month period will trigger a formal investigation, line manager must log this informal meeting and its outcome on College IP
- Three failures in 12 month period – formal investigation following relevant policies/procedures
- These actions are taken to protect the IT systems and data, it can only take one phishing email to put the College at risk of a cyber-attack even with the multilayer security systems already in place, our first and last line of defence against this is our users

17. Social media and websites

17.1 The internet provides a number of social networking opportunities with which users may wish to engage, including for example Facebook, Twitter, blogs and other social media platforms. However, users are expected to behave appropriately, and in ways that are consistent with the College's values, behaviours and policies. All users' online presence and the content of their online presence is their responsibility. Failure to adhere to this may result in Disciplinary action

17.2 When users are contacted by the press about any post on their social networking site that relates them to Huddersfield New College, the Director of Admissions and Marketing must be informed before any response is made.

17.3 All users should be considerate to their colleagues/peers and should think very carefully about the information they post about others and must not post information when they have been asked not to. They are also required to remove information about a colleague/peer if that colleague/peer asks them to do so.

17.4 As a College, we will respond to online legitimate criticism, where appropriate. All reports must be made to the Marketing Department.

17.5 It should always be clear to users whether the site they are interacting with is a Huddersfield New College page run by the College for Huddersfield New College purposes or whether this is a personal page run by an individual for their own private purposes. For example, a staff member's personal profile should not have a URL that contains a Huddersfield New College brand.

17.6 Wiki Sites and Online Encyclopaedia's - the Marketing department is responsible for the writing, overseeing, monitoring and updating of the College's entry on free online encyclopaedia's in association with the Senior Leadership Team. Other users are not permitted to write or edit the College's entry.

17.7 Staff who plan to or already have an internet or digital presence (e.g. personal blog or social media) which indicates in any way that they work at Huddersfield New College, should discuss any potential conflicts of interest with the College's Human Resources team. If an employee is offered payment to produce a blog or other digital item for a third party this could constitute a conflict of interest and must be discussed with the College's Human Resources team.

18. Education and Training

18.1 With the current nature of internet access, it is impossible for the College to eliminate all risks for users. It is our view therefore that the College should support all stakeholders to stay safe online through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

18.2 Within classes, students will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

19. Monitoring compliance

19.1 This Policy and its implementation are subject to internal monitoring and auditing throughout the College, and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The College will also undertake appropriate benchmarking and may be audited by external bodies

20. Linked Documentation

- Internet Provider (JANET) Acceptable Usage
- Data Protection and related Policies
- Safeguarding and Child Protection Policy
- PREVENT procedures
- Student Images Statement (Filming and Student Images Protocol)

21. Disciplinary Procedures

21.1 For any user/stakeholder who is alleged to have committed an act or acts of misconduct under this policy, the relevant College Disciplinary Procedure or Behaviour for Learning Policy and Procedures may be invoked. Such conduct may be treated by the College as a potential act of gross misconduct or a severe breach of our expected behaviours and be subject to formal action. If a breach of statutory legislation occurs, legal action may also be instigated.

21.2 The IT Services team can at any time temporarily suspend a user's access to the network if any unacceptable use has been made or is suspected this will be done in the agreement with the investigating officer/HR team/progress tutor team as relevant. Appropriate actions will be taken according to the level of misuse.

21.3 The IT Services team may remove data/files/communications from user accounts if they believe that unacceptable use has occurred this will be done in the agreement with the investigating officer/HR team/progress tutor team as relevant

21.4 The College reserves the right to use the content of any user's IT activity in any disciplinary process or provide this to any legal body if required to do so by law.

22. Review, publication and communication

22.1 The Senior Leadership Team will review and approve the policy. Once approved, the policy will be published on the College VLE (Moodle) and the College website. Any changes will be communicated via

Staff News. The policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or security incidents that have taken place.

22.2 Only major, significant changes will create a need for current staff to re-sign. All new staff sign the policy as part of their appointment to role.

23. Equality Impact Assessment (EIA)

23.1 The full Equality Impact Assessment is held by HR

24. General Data Protection Regulations (GDPR)

24.1 Information provided to HNC in relation to this policy is processed for the purpose of performance of the employment contact, to enable us to comply with our obligations and exercise our rights as an employer and to enable our employees to exercise their rights as employees. The information will be accessed by HR for the purposes of managing and monitoring employees.

Version	Date	Policy Owner	Comments	Approval Route and Date	Date of Next Review	Equality Impact Assessment Completed (Y/N)
1	May 2012	Julie France			-	N
2	March 2016	Joe Norton and Rebecca Sutcliffe	Updated policy to reflect additional requirements in line with the PREVENT Duty and changes to the College's Firewall settings	Systems Group March 2016	March 2017	Y
3	May 2017	Julie Pryce with College Systems Group	Incorporate separate and overlapping policies (staff IT acceptable use, student IT acceptable use, E-safety, Social Networking)	SLT approval 28th June 2017	March 2019	
4	May 2018	Julie Pryce with College Systems Group	Early review to incorporate GDPR requirements	SLT May 2018 (AWS)	May 2019	
5	March 2019	Julie Pryce with College Systems Group	Updates to policy including incorporating college structure changes	SLT May 2019	May 2021	

6	April 2020	Rebecca Harris with Julie Thomas	Early updates to include video conferencing guidance for remote working	Julie Thomas April 2020	May 2021	
7	Nov 2020	Rebecca Harris with Julie Thomas	Early updates to include references to the Terrorism Act 2006 and minor clarifications surrounding online presence – not a significant change requiring current staff to sign	SLT 16th Dec 2020 (published March 2021)	May 2023	Y
8	May 2023	Rebecca Harris with Maria Dean, Hayley Doyle, Prevent & Online safety group and Data protection & security group	Full review with defined headings added and to incorporate BYOD policy, Password Management (moved from Document 13 - HNC IT Security Framework - Password Management Procedure), Privacy & Website (Cookies) (moved from Separate Privacy and Cookies Policy)	SLT	May 2024	Y

Appendix A – Examples of illegal activity - This list is not exhaustive

Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse imagery
- Child sexual abuse/exploitation/grooming
- Terrorism
- Encouraging or assisting suicide
- Offences relating to sexual images i.e., revenge and extreme pornography
- Incitement to and threats of violence
- Hate crime
- Public order offences - harassment and stalking
- Drug-related offences
- Weapons / firearms offences
- Fraud and financial crime including money laundering

Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990):

- Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)
- Gaining unauthorised access to the college networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)
- Download or distribution of any pirated software

Appendix B – Examples of unacceptable activity - This list is not exhaustive

Users shall not undertake activities that are classed as unacceptable to the college:

- Accessing inappropriate material/activities online at the college e.g. pornography, gambling, drugs.
- Promotion of any kind of discrimination
- Using college systems to run a private business
- Using systems, applications, websites, proxy sites or other mechanisms that bypass the filtering or other safeguards employed by the college
- Infringing copyright
- Unfair usage (downloading/uploading/streaming large files that hinders others in their use of the internet)
- Attempting to access or accessing the college network, using another user's account or allowing others to access college network by sharing username and passwords
- Corrupting or destroying the data of other users or causing deliberate damage to hardware or software
- Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature
- Unauthorised downloading or uploading of files or use of file sharing
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act
- Deliberate actions to breach data protection or network security rules
- Unauthorised use of digital devices (including taking images)
- Unauthorised use of online services
- Using personal e-mail/social networking/messaging to carry out digital communications for college business