IT Acceptable and Safe Use Policy – November 2020

1.0 Introduction

1.1 Use of IT systems is subject to the provisions of all Data Protection regulations, 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 the latest 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.

2.0 Scope of policy

2.1 The following policy applies to all employees, temporary staff, students, governors and visitors (hereafter referred to as users) of the College 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. This also applies to all users utilising their own devices during college working hours.

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 e-safe and to satisfy our wider duty of care.

3.0 Roles and responsibilities

3.1 There are clear lines of responsibility for IT acceptable usage, PREVENT and e-safety within the College. This responsibility sits with the College Systems group, within this group are the senior staff responsible for all areas of IT & ILT. The College's Safeguarding Team contribute to the PREVENT and e-safety element of this policy. The Data Protection & Security group are responsible for keeping up-to- date with new technologies and their use, as well as attending relevant training. It is the group's responsibility to review and update this Policy, 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 e-safety within the College community.

3.2 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 e-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.

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 e-safety. All digital communications must be professional, in line with College policies, and lawful at all times.

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

3.4 Students know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their Progress Tutor. Where any report of an e-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.

Students 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 e-safety lessons as part of the tutorial programme and they are expected to know and act in line with other relevant college policies such as those detailed in section 12. All relevant policies are available to access and download from the College's VLE (Moodle).

Students must electronically sign a reference to this policy which is stored within CEDAR (Student Record Portal). All digital communications must be professional, in line with College policies, and lawful at all times.

4.0 IT Systems usage and monitoring

4.1 IT systems are provided to allow you to perform your work or study related duties. Whilst the College provides a reasonable level of privacy, users should be aware that any usage of the College's IT systems or credentials/authentication remains the property of the College; this may be stored data, emails, images etc.

4.2 The College may 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.

4.3 Computers, electronic devices, storage, credentials/authentication and email accounts are the property of the College and are designed to assist in the performance of your work or study. All users should have no expectation of privacy in any email sent or received, whether it is of a business or personal nature. College email is primarily provided for your use in performing your College duties and personal use should be avoided where possible. The content of email messages and data storage will be monitored. College emails should be kept secure by not setting forwarding rules to other email accounts.

4.4 For business continuity purposes, the College may need to check the emails of employees who are absent.

4.5 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.

Access to online gambling sites is prohibited in accordance with this policy.

4.6 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.

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 in accordance with the College's Disciplinary Procedure, the Student Code of Conduct and/or legal action. 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.

4.7 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.

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.

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.

4.8 For Governors, 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.

4.9 Copies of emails 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.

4.10 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.

4.11 Web filtering will be reviewed periodically to make sure its meets with the PREVENT Duty and other Government advice provided by the Department for Education or National Centre for Cyber Security.

4.12 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).

4.13 Any attempts to disable, defeat or circumvent any of the College's IT systems or credentials/authentication will be treated as a potential act of gross misconduct and will be subject to the College's Disciplinary Procedure, the Student Code of Conduct and/or legal action.

4.14 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.

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

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.

4.16 All users are required to manage folders appropriately and delete any unwanted items, or archive them to the College's OneDrive. It is recommended that files containing personal information that are over three years old are not retained.

4.17 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.

4.18 Staff and governor emails will be stored on the college mail server for 36 months. Automatic deletion at this point will take place on the mail server regardless if the user has utilised the archive facility or saved the email to folder within the mailbox.

4.19 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.

4.20 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).

4.21 Students who have left or completed education at Huddersfield New College; Home drive files will be kept for 1 year before absolute deletion (this satisfies vocational requirements regarding the retrieval of work).

4.22 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).

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

4.23 All actual and suspected security incidents are to be reported to the Director of IT (Infrastructure and Technical Services) immediately who will determine the nature or need of any escalation.

5.0 Social media and websites

5.1 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

5.2 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 Marketing, Admissions and Schools Liaison must be informed before any response is made.

5.3 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.

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

5.5 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.

5.6 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.

6.0 Copyright and downloading

6.1 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.

6.2 Copyrighted software must never be downloaded and installed on any College device.

6.3 All users must not download or distribute any pirated software using the College system. Any such action is likely to be considered as a potential act of gross misconduct and the College's Disciplinary Procedure or Student Code of Conduct will apply.

7.0 Data Protection and sharing information electronically

7.1 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.

7.2 All College mobile devices such as a laptop must be password protected. No data should be stored locally.

7.3 Please refer to the College website which has an area dedicated to Data Protection for full details https://huddnewcoll.ac.uk/about-us/our-policies/data-protection

7.4 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.
- 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.
- 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.
- No sensitive information or personal information should be sent via email to either 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 using the College procedure available on Moodle.
- 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.

7.5 Mobile working/Remote Access

- Information should only be stored on College systems or if remote working is required, remote access or OneDrive should be used.
- The use of Microsoft Remote Apps is available on request to staff only via a Cedar ticket to IT Support. This give access to secure network file storage and secure shared areas.
- Devices should be screen locked when unattended.
- 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 HTTP**S** not HTTP.
- Turn off Wi-Fi on devices when not being used in a public place to avoid automatic connection to open networks.

8.0 Security

8.1 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 up to date. 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.

9.0 Use of images, captures or videos (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.

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.

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 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)
- Students should turn off their video camera before joining the conference - you don't need to see what they are doing/wearing or where they are

- 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

10.0 Education and Training

10.1 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 e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

10.2 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.

11.0 Use of College Equipment Signed out on Loan

11.1 All users utilising loaned IT equipment which is the property of Huddersfield New College, should be aware it should only to be used in conjunction with College business and is also covered by this acceptable and safe use policy.

11.2 Any person responsible for a loaned IT device must undertake to be responsible for the equipment. They must commit to returning the equipment to the IT Services Office on the agreed return date or the end of their contract (whichever is earliest). This is subject to a signed loan agreement. The equipment must be returned in the same condition as when it was issued.

11.3 The Human Resources (HR) and the IT Services teams hold records for College equipment loaned to users.

12.0 Linked Documentation

- Internet Provider (JANET) Acceptable Usage
- Data Protection and related Policies
- Safeguarding and PREVENT Policies

13.0 Disciplinary Procedures

For any stakeholder who is alleged to have committed an act or acts of misconduct under this policy, the relevant College Disciplinary Procedure or Student Code of Conduct may be invoked. If a breach of statutory legislation occurs, legal action may also be instigated.

14.0 Review, publication and communication

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 bienially. 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.

IT Acceptable and Safe Use Policy – November 2020

Version	Date	Policy Owner	Comments	Approval Route and Date	Date of Next Review	Equality Impact Assessment
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