IT Acceptable and Safe Use Policy

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, 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 the College BYOD provision 'HNC-Guest Wi-Fi'. This also applies to all use of the internet and other forms of electronic communication such as email, mobile phones and social media sites.

2.2 Our approach is to implement appropriate safeguards within the College which supports all employees, temporary staff, students, governors and visitors 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 all employees, temporary staff, students, governors and visitors 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 College Systems group are responsible for keeping up-to- date with new technologies and their use, as well as attending relevant training. It is the College Systems 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 College Systems group via a Cedar helpdesk ticket. 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 at all times.

3.3 Visitors would be expected to report any concerns to Reception, who will inform the College Systems group. Visitors electronically sign into the college on entry and have to read, acknowledge and electronically sign, agreeing to our expectations.

3.4   Students must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be their progress tutor or the pastoral team in the Learning Resource Centre or 502.   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. 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 at all times.

4.0   IT Systems usage and monitoring

4.1   The 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 remains the property of the College; this may be stored data, emails, images etc.

4.2   The College may monitor any aspects of its computer systems that are made available to any user and may also monitor, intercept and/or record any communications made, including telephones, email 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 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.

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.

4.6   It is forbidden to use email and the internet in order to access, download and/or transmit any material which might reasonably be considered obscene, abusive, sexist, racist, extreme, radical and/or defamatory. Similarly, access to online gambling sites is prohibited in accordance with this policy. All users should be aware that such material may also be contained in jokes sent via email. Such conduct may be treated by the College as a potential act of gross misconduct or a severe breach of our Student Code of Conduct. The College reserves the right to use the content of any user's IT activity in any disciplinary process.

All users must not make derogatory remarks in electronic communications about colleagues, employees, students, competitors or any other person. Any written derogatory remark may constitute libel and be subject to formal action in accordance with the College's Disciplinary Procedure, the Student Code of Conduct and/or legal action.

4.7   For employees, 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.

4.8   For Governors, any information regarding specific details of college business or employees 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   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 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.

4.11   The 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 computer security facilities 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. Further details are given in the Password Policy which should be read in conjunction with this Policy.

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

        When employees 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   Employees who plan to or already have an internet presence (e.g. personal blog) 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 for a third party this could constitute a conflict of interest and must be discussed with the College's Human Resources team.

4.18   Employee 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   Employees, temporary staff and governors whose contracts (or terms of engagement) have ceased; emails and Home drive files will be kept for 12 months before absolute deletion.

4.20   Employees, temporary staff and governors whose contracts (or terms of engagement) 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   Employees, temporary staff, students, governors and visitors using or administering the IT facilities 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 and 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 Huddersfield New College staff and students may wish to engage, including for example Facebook, Twitter, blogs and other social media platforms. However, when someone clearly identifies their association with Huddersfield New College and/or discusses their work, they are expected to behave appropriately when on the Internet, and in ways that are consistent with the College's values and policies.

5.2   All employees, temporary staff, students, governors and visitors who identify themselves as part of Huddersfield New College:
- o   Must not engage in activities on the Internet which might bring Huddersfield New College into disrepute
- o   Must not use the Internet in any way to attack or abuse students, colleagues, teachers or tutors
- o   Must not post derogatory or offensive comments on the Internet

5.3   When employees, temporary staff, students, governors are contacted by the press about any post on their social networking site that relates them to Huddersfield New College, the Director of Marketing and Schools Liaison must be informed before any response is made.

5.4   All employees, temporary staff, students, governors 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.

5.5   As a College, we should respond to online legitimate criticism. We should not remove derogatory or offensive comments but must report them to the relative administrators, which will be members of the Marketing

Department for most instances and the Senior Leadership Team for issues considered to be of a highly serious and/or sensitive nature.

5.6   Blogs or websites that are purely about personal matters and do not identify the blogger as a Huddersfield New College employee or do not discuss the College, will normally fall outside the guidance set out in this policy.

5.7   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.

5.8   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 employees, temporary staff, students, governors 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 employees, temporary staff, students, governors and visitors 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 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 personal or college 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
    a. 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.

b. 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.

c. College owned removable media must be formatted or destroyed by the IT Support team only.

d. 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.

e. 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.

f. 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.

g. 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

a. Information should only be stored on college systems or if remote working is required, remote access or OneDrive should be used.

b. The use of Microsoft Remote Apps is available on request to employees only via a Cedar ticket to IT Support. This give access to secure network file storage and secure shared areas.

c. Devices should not be logged-on and unlocked when unattended.

d. Users shall ensure that unauthorised persons (friends, family, associates, etc.) do not gain access to mobile systems, devices or information in their charge.

e. 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.

f. Turn off Wi-Fi on devices when it is 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.

IT Acceptable and Safe Use Policy

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 employees, temporary staff, students or governors.

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 for their professional development.

9.4   The College has various video calling/conferencing platforms recommended which can be used as a learning tool in the event that the college is in a period of remote working, however the guidance below should be followed
   o   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
   o   As the host if you record your video call/meeting, 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
   o   Never arrange one to one video meetings with students for safeguarding reasons
   o   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)
   o   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
   o   You should only ask students to turn their camera on (not in a 1-1 situation) if the subject visually requires it e.g. to view an art piece
   o   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!
   o   Be respectful of other users in the language that you use and your behaviour on the video call/conference
   o   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 employees, temporary staff, students, governors and visitors. 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

IT Acceptable and Safe Use Policy

11.1   All employees, temporary staff, students, governors and visitors 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 Support 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/or IT Network teams hold records for college equipment loaned to employees, temporary staff, students, governors and visitors.

12.0   Linked Documentation

- Internet Provider (JANET) Acceptable Usage
- Password Policy
- 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 may be invoked. If a breach of statutory legislation occurs, legal action may also be instigated.

14.0   Review

This Policy will be reviewed biennially. Any signed versions of this policy will be applicable to any updated policies when published to staff.

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 2020 | |
| 6 | April 2020 | Rebecca Harris with Julie Thomas | Updates to include video conferencing guidance for remote working | Julie Thomas April 2020 | May 2020 | |

INTRODUCTION
The purpose of carrying out an Equality Impact Assessment (EIA) is to provide the basis for creating equality objectives and performance indicators that will drive improvement and change in ensuring the College meets the needs of different groups of people with different protected characteristics, as defined in the Equality Act 2010.

What is an impact assessment?
An EIA is a systematic and thorough consideration of how every aspect of the College's functions (i.e. policies, procedures, practices and plans) is affecting, or is likely to affect different people. EIAs should be reviewed a part of a rolling programme and the Action Plan updated accordingly.

It is good practice to carry out EIAs, although they are no longer mandatory. When conducting EIAs must explicitly consider impact on students, staff and other key groups in terms of race, disability, gender (including gender identity), sexuality, age, and religion and belief, and publish the results. Consultation with customers and potential customers, external clients, staff and students will be part of the EIA procedure and will also link to the Self-Assessment Report (SAR) and strategic plan for the College. The involvement of different stakeholders will evidence our commitment to embedding equality and diversity within all our services and the curriculum. The EIAs will be led and monitored by the Assistant Principal – People and Place.

What needs to be impact assessed?
The EIA process will encompass all policies, procedures, practices and plans. When and where these are identified, each will need an EIA or review as part of a rolling programme, to determine whether they have a differential impact in relation to equality.

Findings of EIAs
The findings of an EIA may provide a number of possible outcomes:

1.   The EIA shows that employment practices or services have a different impact measured by one or more protected characteristic.
2.   The EIA shows a different impact which is demonstrated to be adverse impact.
3.   The EIA shows no differential impact in employment practices or service delivery.
4.   There is insufficient evidence to judge whether there is differential impact.
5.   The EIA indicates that there are needs that are not being met.

Can I assess my own policies, procedures, practices and plans?

IT Acceptable and Safe Use Policy

EIAs will usually be completed by the owner of the policy, procedure, practice and plan in conjunction with another colleague who is familiar with the process of conducting EIAs. The nominated person should not be involved with the design, maintenance or enforcement of the policy, plan, practice or procedure. This is to ensure that the EIA process is objective and robust, as a neutral party is more likely to highlight elements that will lead to positive change.

Part One – The Impact Assessment

Date of last assessment (if applicable)	-
Date this assessment commenced	19/03/2019
Name of policy/procedure/practice/plan being assessed	IT Acceptable Use Policy
Name and job title of policy/procedure/practice/plan owner	College Systems Group
Name(s) of independent colleague(s) appointed to contribute to the assessment	Joe Norton, Director of TLA (Digital Learning Technologies)
Is this a new or existing policy/procedure/practice/plan?	Minor changes to incorporate college structure changes

INITIAL SCREENING

1. **Please summarise the main aims of the policy/procedure/practice/plan. Include the intended benefits.**	The principal aim of the policy is to ensure safe and secure use of college systems and equipment, safeguarding users and all college users.
2. **What consultation has been undertaken in the development of the policy/procedure/practice/plan?**	The policy has been referred to the College's Systems Group and members of the Senior Leadership Team for approval, and is based on the JISC recommended staff usage policy, and as such follows national guidelines and legal regulations.
3. **What evidence, data or information is available to indicate how the policy/procedure/practice/plan might affect equality?**	There is no evidence to suggest that this policy will have any adverse differential impact on equality. The policy applies to employees, temporary staff, students, governors and visitors equally.

IT Acceptable and Safe Use Policy

| 4. In what areas could the policy/procedure/practice/plan have a significant adverse differential impact?

If you have selected one or more boxes for question 4, please go straight to question 5.

If you have not selected any of the boxes for question 4 there is no need to complete the rest of this documentation. However, you must write the reasons why you believe there will be no differential impact, in respect of any of the protected characteristics listed, in the space opposite. | **Disability** ☐
Race ☐
Gender (including Gender Identity) ☐
Sexual Orientation ☐
Age ☐
Religion or belief ☐

See point 3. | |

ASSESSING IMPACT AND STRENGTHENING THE POLICY/PROCEDURE/PRACTICE/PLAN

5. What general concerns are there that the policy/procedure/practice/plan could have a differential impact on the protected characteristics you have indicated in question 4? Please give details. What relevant evidence is available to support these concerns? Please use data/statistics where possible.	None
6. What are the risks associated with the effectiveness of the policy/procedure/practice/plan in relation to the differential impact?	None
7. What are the expected benefits of the policy/procedure/practice/plan?	To satisfy legal compliance and for the maximum security of systems, information and data
8. Who are the 'interested parties' (i.e. adversely affected groups) in relation to this policy/procedure/practice/plan?	All users are interested parties but none are adversely affected

IT Acceptable and Safe Use Policy

9. How will these interested parties be consulted and communicated with?	All users must comply due to the legal implications. Training will be given and users are required to sign to acknowledge acceptance of adherence to the policy.
10. Which relevant experts and/or equality groups have been approached to explore the issues with which the policy/procedure/practice/plan is concerned? How have the views of these experts/groups been sought? (Please be as specific as possible, e.g. by letter, meetings, interviews, workshops, questionnaires, or any other method.)	College systems group, NORVIC groups, JiSC
11. Please give details of the views of the experts/groups on the issues involved.	All incorporated in the amended policy
12. Taking into account these views, and the available evidence, please outline the risks associated with the policy/procedure/practice/plan weighed against the benefits.	None
13. What changes/modifications will now be made to the policy/procedure/practice/plan in the light of this Impact Assessment?	None
14. How will these changes/modifications be communicated to interested parties (i.e. the groups which were adversely affected) and those consulted? (This should form part of the Action Plan.)	As item 9
Signed (completing officer 1)	**Print Name and Job Title** **Rebecca Sutcliffe, Director of IT (Infrastructure & Technical Services)**
Signed (completing officer 2)	**Print Name and Job Title** **Julie Pryce, Assistant Principal Curriculum Data and Planning**
Date of completion of Impact Assessment	**19/03/2019**

IT Acceptable and Safe Use Policy

Actions arising from screening										
(R = Race/Ethnicity, R&B – Religion and Belief, D – Disabled People, G – Gender (including gender identity), SO – Sexual Orientation, A – Age)										
R	R&B	D	G	SO	A	Action Required	By Whom	By When	Intended Outcome	Change resulting from EIA and date (include evidence if possible)

IT Acceptable and Safe Use Policy