HTP Apprenticeship College

IT Policy

Contents

1. Introduction

1.01 Background

Digital technologies have become integral to the lives of many people in today's culture. The internet and other information technologies are powerful tools which open up new opportunities for everyone therefore all users have a right to safe use of IT access at all times.

However, the use of these new technologies can put users at risk. Some of the dangers include:

- Exposure to extremist, radical and/or terrorist materials.
- Access to illegal, harmful or inappropriate images or other content.
- Loss of privacy / control of personal information.
- Grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge.
- Inappropriate communication / contact with others, including strangers.
- Cyber-bullying.
- Access to unsuitable video / internet games.
- An inability to evaluate the quality, accuracy and relevance of information on the internet.
- Plagiarism and copyright infringement.
- Illegal downloading of music or video files.
- Hacking, viruses and system security.
- The potential for excessive use which may impact on the social and emotional development and learning.

As with all other risks, it is impossible to eliminate the risks completely. By providing good examples and role models and by raising awareness, it is possible to build the resilience of for all, so that they have the confidence and skills to deal with these risks. Every person needs to be aware of the risks posed by inappropriate use.

Many of these risks reflect situations online and it is essential that this IT Policy is used in conjunction with other policies such as The Safeguarding Policy.

1.02 Introduction and Policy Statement

The HTP Apprenticeship College IT Policy provides a simple framework to ensure the necessary safeguards are in place to maintain protection, security and safety of for all within legislation and protecting confidentiality. This policy covers the usage and access to the HTP Apprenticeship College network and the internet across all campus sites.

1.03 Purpose of Policy

The intention of this policy is to ensure:

- All hardware and software systems information systems at HTP Apprenticeship College are protected from security threats and to mitigate risks that cannot be directly countered.
- All users are aware of and are able to comply with relevant UK and EU legislation and regulation.

- All users are aware of and understand their personal responsibilities to protect the confidentiality and integrity of the data that they access.
- All users are aware of and are able to comply with this policy and other supporting policies.
- The safeguarding of HTP Apprenticeship College's reputation and business by ensuring its ability to meets its legal obligations and to protect it from liability or damage through misuse of its IT facilities.
- Timely review of policy and procedure in response to feedback, legislation and other factors so as to improve ongoing security.

1.04 Scope

The HTP Apprenticeship College IT Policy applies to all HTP Apprenticeship College IT systems. This policy also applies to all persons accessing and using the HTP Apprenticeship College networks, VLE's, hardware, software / applications, phone systems and the internet.

2. Policy

2.01 Definition

The following HTP equipment protected under the IT Policy includes:

- Desktops PC’s – Issued or provided to staff to carry out their duties.
- Laptops / Tablets – Issued or provided to staff to carry out their duties.
- Phones – Telephones/Voice Communication hardware allocated to each member of staff to carry out their duties including desk phones, soft phones and mobile phone app
- Media/Portable Media – Electronic storage devices such as DVDs, CDs, USB memory sticks and hard drives issued or provided to staff and to carry out their duties.
- Mobile phones – issued or provided to staff to carry out their duties.
- External Communications Infrastructure – Equipment used to connect to the HTP Apprenticeship College network and/or the internet.
- All related IT Facilities used in campus training rooms.
- Equipment issued or provided to learners to undertake their college work including laptops, tablets and PC’s.
- Equipment issued or provided to external stakeholders to undertake activities relating to college based programmes.

The persons defined as ‘all’ in this IT Policy include:

- HTP staff – including full-time, part-time, seconded/secondees, volunteers, sub-contracted, agency, work experience and contractors.
- HTP learners – including applicants, learners on any funded or non-funded programme with HTP Apprenticeship College, based at the campus and/or based at an employer site.

All users are required to understand the IT Policy. Dissemination of the IT Policy is carried out in the following ways:

Who?	How?
Learners	Policy available on Myhtp and htp.ac.uk Prevent awareness will be included in learner Induction sessions, formal teaching sessions, learner reviews, resources such as participation in Prevent and the British Values related student activities
Staff	Policy available on Myhtp / Myhtp-Staff and htp.ac.uk Staff induction, receive mandatory training and updates. ‘All Staff’ e-mails, team meetings and staff newsletters
Managers / Directors / Governors	Policy available on Myhtp / Myhtp-Staff and htp.ac.uk Staff induction, receive mandatory training and updates. ‘All Staff’ e-mails, team meetings and staff newsletters SMT / Governors meeting updates regular discussions as appropriate

2.02 Awareness and Communication

All authorised users will be informed of the HTP Apprenticeship College IT Policy and other relevant supporting policies when their account login is issued or when access is authorised to the HTP Apprenticeship College networks and/or the internet. Conforming to the IT Policy is mandatory and updates to this policy will be confirmed by the Safeguarding Officer for IT. The policy will be reviewed annually or more frequently to reflect changes in legislation and regulation. Regular discussions will take place with all users to check comprehension. This will occur at staff induction, team meetings and training days and with learners in the workplace and in the classroom. Employer and other users will also be updated of changes.

2.03 Legislation and Regulation

HTP Apprenticeship College and all users must adhere to all current UK and EU legislation as well as regulatory and contractual requirements. These include the following:

Computer Misuse Act 1990	http://www.legislation.gov.uk/ukpga/1990/18/contents
Data Protection Act 1998	https://www.gov.uk/data-protection
General Data Protection Regulation (GDPR) 2018	https://eugdpr.org/
The Freedom of Information Act 2000	http://www.legislation.gov.uk/ukpga/2000/36/contents
Copyright, Designs and Patents Act (CDPA) 1988	http://www.legislation.gov.uk/ukpga/1988/48/contents
Counter-Terrorism and Security Act (CTSA) 2015	http://www.legislation.gov.uk/ukpga/2015/6/contents
Human Rights Act 1998	http://www.legislation.gov.uk/ukpga/1998/42/contents
Obscene Publications Act 1964	http://www.legislation.gov.uk/ukpga/1964/74/contents
Protection of Children Act 1999	http://www.legislation.gov.uk/ukpga/1999/14/contents
Health and Safety Act 1974	http://www.legislation.gov.uk/ukpga/1974/37/contents
Police and Justice Act 2006	http://www.legislation.gov.uk/ukpga/2006/48/contents
Terrorism Act 2006	http://www.legislation.gov.uk/ukpga/2006/11/contents
Digital Economy Act 2010	http://www.legislation.gov.uk/ukpga/2010/24/contents
Defamation Act 2013	http://www.legislation.gov.uk/ukpga/2013/26/contents

2.04 Preventing Extremism and Radicalisation

HTP Apprenticeship College take their responsibility to ensure all IT users are in a safe, secure and work in a healthy environment seriously. HTP Apprenticeship College recognise that extremism and exposure to extremist materials and influences can lead to poor outcomes for learners. We further recognise that if extremist views are unchallenged, HTP Apprenticeship College are failing to protect a ll users from potential harm.

HTP Apprenticeship College strictly adheres to the Government's Prevent Strategy in all its activities, this may be accessed via the following link:
https://www.gov.uk/government/publications/prevent-duty-guidance
HTP Apprenticeship College endeavours to incorporate these duties in a way that does not;

(a) Stifle legitimate discussions, debate or student engagement activities in the local community; or
(b) Stereotype, label or single out individuals based on their origins, ethnicity, faith and beliefs or any other characteristics protected under the Equality Act 2010.

Prevent is one of 4 strands of the Government's counter terrorism strategy – CONTEST. The UK currently faces a range of terrorist threats. Terrorist groups who pose a threat to the UK seek to radicalise and recruit people to their cause. Prevent happens before any criminal activity takes place by recognising, supporting and protecting people who might be susceptible to radicalisation through the use of the internet including social media.
Therefore early intervention is at the heart of Prevent which aims to divert people away from being drawn into terrorist activity. The HTP Apprenticeship College IT Policy will:

- Ensure all users of IT have an awareness and understanding of Prevent.
- Provide a clear framework to structure and inform our response to safeguarding concerns for IT use, including a supportive referral process for those who may be susceptible to the messages of extremism.
- Embed the British Values into the curriculum and ways of working.
- Recognise current practice which contributes to the Prevent agenda.
- Identify areas for improvement linked the HTP Self-Assessment process.
- Respond to the ideological challenge of terrorism and aspects of extremism, and the threat we face from those who promote these views online.
- Provide practical help to prevent people from being drawn into terrorism and violent extremism through training, monitoring and resources to ensure all users are given the appropriate advice and support.
- Work with learners and employers across all delivered sectors to ensure comprehension of risks of radicalisation online which need to be addressed.
- Promote and reinforce shared values, including the British Values to create space for free and open debate; and to listen and support the user's voice.
- Breakdown segregation among different learner communities including by supporting inter-faith and inter-cultural dialogue and understanding online including social media; and to engage all users in playing a full and active role in wider engagement in society.
- Ensure student safety of all users online and that HTP Apprenticeship College is free from cyberbullying, harassment, discrimination, extremist views and radicalisation.
- Provide support for all users who may be at risk of radicalisation and signpost to appropriate sources of advice and guidance.
- Ensure that learners and staff are aware of their roles and responsibilities in preventing violent and non-violent extremism.

The definitions below relate to an ideology / set of beliefs:

- **Radicalisation** is the process by which a person comes to support terrorism and forms of extremism that may lead to terrorism.
- **Safeguarding** is the process of protecting vulnerable people, whether from crime other forms of abuse or from being drawn into terrorism-related activity.
- **Terrorism** is an action that endangers or causes serious violence, damage or disruption and is intended to influence the government or to intimidate the public and is made with the intention of advancing a political, religious or ideological view.

- **Vulnerability** describes factors and characteristics associated with being susceptible to radicalisation.
- **Extremism** is vocal or active opposition to **British Values**, including ‘democracy’, ‘the rule of law’, ‘individual and mutual respect’ and ‘tolerance of different faiths and beliefs.’

2.05 Managing Risks and Responding to Events

HTP Apprenticeship College will ensure that it monitors risks associated with the use of IT and that it is ready to deal appropriately with issues which arise through the following:

- Understanding the nature of threat from violent extremism and how this may impact directly and indirectly on HTP Apprenticeship College.
- Identifying, understanding and managing potential risks from external influence.
- Responding appropriately to events reported via local, national or international news that may impact on all users.
- Ensuring plans are in place to minimise the potential for acts of violent or non-violent extremism within the College.
- Ensuring measures are in place to respond appropriately to a threat or incident at HTP Apprenticeship College and the learner workplace.
- Continuously developing and reviewing the HTP Apprenticeship College IT Policy and other related policies to ensure full compliance.

2.06 Responsibility

The HTP Apprenticeship IT Policy is an integral part of the Safeguarding Policy and should be seen as an extension to our established safeguarding procedures.

All IT users have a responsibility to:

- Create and support an ethos that upholds HTP Apprenticeship College’s mission, vision and values including the British Values, to create an environment of respect, equality and diversity when using IT.
- Participate in training when required in order to have the skills to recognise those who may be vulnerable to radicalisation, involved in violent or non-violent extremism, and to know the appropriate action to take if they have concerns.
- Report any concerns around extremism or radicalisation via the safeguarding reporting channels.
- Report literature displayed around at HTP Apprenticeship College and/or the learners workplace that could cause offense or promote extremist views.
- Participate in engagement with local communities, learner workplace and external organisations as appropriate.

2.07 Appropriate use

All HTP Apprenticeship College equipment must be used in a responsible manner and within legislation at all times. IT Users must not misuse the technology by taking any action which could bring HTP Apprenticeship College into disrepute, cause offence, interfere with the work of, or jeopardise, the security of data, networks, equipment or software.

- The facilities are primarily for business use by staff and for learners to complete activities, exams and access resources and carryout research.
- The guiding principle is that, despite its immediacy and ease of distribution, electronic communication and information should be treated no differently from that on paper.
- HTP Apprenticeship College has a responsibility to ensure misuse is not taking place. Contents of mail and files may be monitored, the contents of which will remain confidential, unless they contravene the IT Policy.
- Adherence to this policy is a condition for using the equipment and networks of HTP Apprenticeship College.
- Failure to comply with the IT Policy is a serious disciplinary offence, which will lead to action being taken. It could also lead to criminal or civil. HTP Apprenticeship College will report all illegal offences to the police.
- IT users are not permitted to modify the general settings on the computer or applications in such a way that others would have difficulty in using the equipment. Neither are they permitted to install any software onto the systems.
- The network / Documents Folder should be used for storage of files (not your PC). These files will be backed-up every day, your PC files will not. Files stored on your laptop should be loaded on to the network as soon as possible for backup.

2.08 Common misuse of IT

The following common misuse of IT is in addition to misuse previously documented in this IT Policy:

Using electronic media for creation, use, transmission or encouragement of material which is:

- Illegal, obscene or libellous.
- Offensive or annoying.
- Defamatory.
- Infringes another person’s copyright.
- Brings HTP Apprenticeship College into disrepute.
- Transmission of unsolicited commercial or advertising material (spamming).
- Obtaining unauthorised access to HTP Apprenticeship College’s or another Organisation’s IT facilities.
- Violating other people’s privacy.
- Using chat lines, social networking sites or similar services, unless for legitimate business use.
- Playing games.
- Illegal activities including breaching the legislation and regulations
- Wasting network and staff time and resources.
- Disrupting other users’ work in any way, including by viruses or data corruption.
- Expressing personal views, this could be misinterpreted or contravene the IT Policy and other HTP Apprenticeship College policies.
- Committing HTP Apprenticeship College to purchasing or acquiring goods or services without proper authorisation.
- Downloading copyrighted or confidential information.

2.09 Offensive and other Illegal Material (text, images and audio)

Offensive material is anything that is pornographic; involves threats or violence; promotes illegal acts, racial or religious hatred, and discrimination of any kind, extremist material and radicalisation. The use of this material will be viewed seriously and the person concerned will face disciplinary proceedings, and where necessary be reported to the appropriate authority, criminal proceedings may follow:

- All IT users are expected to be aware that links of webpages can often link to inappropriate sites. Accidental access will not result in disciplinary action but failure to report it may do so.

- All IT users receiving offensive or sexually explicit mail should immediately report this to a senior member of staff.

2.10 Private use of IT Equipment

HTP Apprenticeship College wishes to encourage the use of the Internet and electronic mail facilities by staff and learners to develop competence and understanding of its potential. Staff and learners may use their Internet connections for occasional private purposes, at the discretion of the teacher or staff line manager, provided:

- It does not interfere with the work tasks and is accessed at times outside of designated hours.
- Staff must not access websites and social media relating to a personal business interest.
- It is not used for commercial purposes including the sale or purchase of goods and services.
- It does not involve the use of newsgroups, chat lines, social networking sites or similar services.
- It complies with this IT Policy, including its provisions regarding misuse.

2.11 Use of Email

All staff must only use their assigned HTP email account (firstname.lastname@htp.ac.uk) to communicate with staff, partners/customers, learners and employers. Staff are not allowed, under any circumstances, to communicate using a personal email account. This breeches safeguarding policies, staff handbook policies and IT Policies.

Email should be regarded as public and permanent. It is never completely confidential or secure and despite its apparent temporary nature, it can be stored, re-sent, and distributed to large numbers of people.

Email must not be used for sending offensive, threatening, defamatory, or illegal material including extremist views to radicalise. Sending email is the same as sending a letter or publishing a document in law, so defamatory comments can result in legal action. Internet email has been used successfully as evidence in libel cases. This includes using e-mail to promote personal views to colleagues or the press relating to disputes.

Email must not be used to harass staff, learners or other recipients. Harassment can take the form of argumentative or insulting message (flame mail) or any other message the sender knows or ought to know would cause distress to the recipient. It is easy to be misunderstood in e-mail. People often treat it like phone calls but forget that the emotional meaning is often lost in text. Humour can be misinterpreted. Email should not be ambiguous;

- Staff and learners should not re-send e-mail chain letters and should use caution with any e-mail that asks the reader to forward it to others.
- Only copy e-mails to those that have immediate need to receive the information. Unless absolutely necessary do not request a confirmation of delivery and reading as this adds to the network traffic.
- All emails must contain a disclaimer at the end of the text.
- The correct form of address is to be used and good practice is to not use capitalisation where possible within the text as this could be deemed as offensive.

2.12 Usage monitoring

HTP Apprenticeship College may monitor the use of the Internet, email and file transfers, which use its equipment or network, irrespective of whether they are for HTP Apprenticeship College or private use. The email content of a member of staff or learners using HTP Apprenticeship College accounts can be monitored with reasonable justification and with the authority of the Chief Executive.

2.13 Security

- **Company Network - The network and its peripherals should be kept** secure under all circumstances. This requires that the all campus sites should always be locked when staff are not present. All computers should be password protected.
- **Use of Portable Equipment -** Every precaution must be taken with portable computer equipment to ensure it is not stolen or damaged. All portable equipment (laptops, tablets, mobile phones) must be retained in the possession of the holder at all times and should not be left un-attended either overnight or off-site.
- If stored in a car all doors, windows and other openings must be closed and securely locked. The property must be hidden from view as far as practical (ideally in the boot of the car).
- It is the IT user's responsibility to follow these precautions at all times or HTP Apprenticeship College's insurance will be invalidated and the employee may be liable for the loss.
- Laptops and phones should be locked to prevent unauthorised access, staff must not change laptop passwords without the permission of the Chief Executive.

2.14 Connections

- All connections to the Internet must be via HTP Apprenticeship College network and its firewall to ensure maximum control and protection.
- Firewall facilities are deployed to protect HTP Apprenticeship college network.

2.15 Virus Protection

- All IT users are required to take all reasonable precautions to avoid computer virus infections.
- HTP Apprenticeship College's virus checking occurs on all PC's using the Internet. IT Users must not disable the virus scanning software.
- Files and e-mail attachments can transfer viruses therefore all servers have online scanning and most viruses are removed on arrival to the site. If your PC has been infected you must report it to a member of staff or IT support staff immediately. Do not continue to use until you are advised of required actions.

2.16 Downloading

- Software (including games and entertainment software*)* **must not** be downloaded from the Internet.
- Music and video files should only be downloaded for legitimate business use or as part of activities set for learners as these files occupy large amounts of storage space on HTP Apprenticeship College network.

This is not an exhaustive list but is an indication of the types of conduct that may result in disciplinary action and possibly summary dismissal or exclusion.

2.17 Social Network Use

The purpose of this section is to provide clear information on your responsibilities as an IT user. It is written for the protection and safeguards all IT users.

The absence of, or lack of explicit reference to a specific website does not limit the extent of the application of this IT policy. Where no policy or guideline exists, all IT users should use their professional judgment and take the most prudent action possible. Consult with your tutor, consultant, line manager or manager/director for clarification on any aspect of this IT Policy.

- When communicating on a social network or similar site, all IT users must be respectful to HTP Apprenticeship College, work colleagues, consultants, tutor, customers, learners, stakeholders, and competitors.
- Any personal blog or entry which makes reference to your work environment should contain a clear disclaimer that the views expressed by the author in the blog are the author's alone and do not represent the views of HTP Apprenticeship College. Be clear and write in the first person. Make it obvious that you are speaking for yourself and not on behalf of HTP Apprenticeship College.
- Information published on your blog(s) should comply with this IT Policy, the HTP confidentiality and disclosure of proprietary data policies. This also applies to comments posted on other blogs, forums, and social networking sites.
- For the avoidance of doubt, you may not publish any image which has been taken at a work related event. This includes evening activities, as well as team building social events.
- All IT users must accept that your online presence reflects the employer/company you work for and HTP Apprenticeship College. Be aware that your actions, captured via images, posts, or comments can reflect that.

- Do not reference or cite customers, clients, learners, business partners, or colleagues without their express consent. In all cases, do not publish any information regarding another person or any of their staff.
- Respect copyright laws, and reference or cite sources appropriately. Plagiarism applies online as well.
- Company logos and trademarks may not be used without written consent of which they belong to. You are not permitted to use HTP Apprenticeship College's logos without permission.
- IT users are obliged to adhere to their responsibilities under this IT Policy and other related policies such as our safeguarding violation under will result in disciplinary action being taken which may result in dismissal or exclusion.
- If you publish any detrimental or derogatory information about HTP Apprenticeship College, its learners, staff or its stakeholders you may be subject to formal disciplinary action being taken against you. Where actions could be considered to be cyber bullying or some similarly serious action, this would be classed as gross misconduct which could result in your dismissal or exclusion.
- Social media activities should not interfere with work tasks. You should not spend any work/classroom time on social media activities. Failure to comply with this standard may result in disciplinary/exclusion action being taken against you. Serious or persistent offences could ultimately lead to dismissal or permanent exclusion.
- Staff must not be 'friends' with learners on social media platforms. Staff and learners must only communicate using the approved methods as detailed in this policy. Failure to comply with this may result in disciplinary/exclusion action being taken against you for breeching safeguarding procedures.

2.18 Online Gambling

Online gambling is not permitted, under any circumstances, using HTP Apprenticeship College equipment and software or any other personal equipment during work/classroom time.

Children may view inappropriate or upsetting content if they play games that aren't suitable for their age. This could include sexual or violent material. It might be in-game content or produced by other players.

Some players can be abusive towards others or try to exclude them from the game. Some players may also hack another user's account or try to steal and destroy their virtual possessions. This can be as upsetting for a young person as if it happened in real life.
Children may play with adults they don't know. People of all ages play games. Some adults may exploit this and try to build an emotional connection with a child for the purpose of grooming.

Some children may find it hard to stop playing games or find that gaming is getting the way of them doing other activities.

Concerns should be reported immediately to a safeguarding officer.

2.19 Reporting

The people at HTP Apprenticeship College who have designated safeguarding roles are:

Name / Role	Contact Details
Nicki Neville Lead Designated Person	Riverbank Campus 01983 824930 / 07795 262724 nicki.neville@htp.ac.uk
Lisa Pilbeam Lead Designated Person	Old Grammar School Campus 01983 533926/07825 133840 lisa.pilbeam@htp.ac.uk
Peter Johnson Designated Person with Responsibility for digital management	Old Grammar School Campus 01983 533926 / 07795 275175 peter.johnson@htp.ac.uk
Di Kennet Designated Person	Old Grammar School Campus 01983 533926 / 07825 199726 di.kennet@htp.ac.uk

Any concerns must be raised with a Designated Safeguarding Person. The Designated Safeguarding Person then will act in accordance with HTP Apprenticeship College's Safeguarding Policy

2.20 Related Policies and Documents

HTP Preventing Extremism and Radicalisation Safeguarding Policy
HTP Safeguarding Young People and Vulnerable Adults Policy
HTP Child Protection Policy
HTP Health and Safety Policy
HTP Equality and Diversity Policy
HTP Bullying and Harassment Policy
HTP Safer Recruitment Policy