Acceptable IT usage policy

1.0 Introduction

1.1 Use of IT systems is subject to the provisions of the Data Protection Act 1998, the Copyright, Designs and Patents Act 1988 and subsequent regulations, and the Computer Misuse Act 1990 as well as college policies.

1.2 In order to comply with the latest legislation, the training provider 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 training provider 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 provider 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 organisation. This responsibility sits with the senior staff responsible who are responsible for all areas of IT & ILT. The organisation are responsible for keeping up-to- date with new technologies and their use, as well as attending relevant training. It is the centre manager responsibility to review and update this Policy, deliver 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 business manager. 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.

3.3 Visitors would be expected to report any concerns to Reception, who will inform centre manager. Visitors on entry and must 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. 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 always act safely and responsibly 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 policies such as those detailed. All relevant policies are available to access and download from the College's VLE (Moodle).

Students must confirm in the induction that they have read all policies which is stored in their portfolio's.

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 organisation provides a reasonable level of privacy, users should be aware that any usage of the IT systems remains the property of the provider; this may be stored data, emails, images etc.

4.2 The provider 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 provider 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 provider 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 provider will need to check the emails of employees who are absent.

4.5 The provider recognises that it may sometimes be necessary for users to carry out personal tasks using the IT facilities (i.e. send/receive personal emails, make/receive personal phone calls and carry out private research on the internet). 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 by email. Such conduct will be treated by the provider as a potential act of gross misconduct or a severe breach of our Student Code of Conduct. The provider 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 providers Disciplinary Procedure, the Student Code of Conduct and/or legal action.

4.7 For employees, use of the standard college email signature is strongly recommended.

4.8 For Governors, any information regarding specific details of provider business or employees must be communicated using the organisation 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 All users are responsible for safeguarding their password for the providers IT systems. For reasons of security, individual passwords should not be printed, stored online or given to others.

4.11 When users leave the organisation/provider their access rights to all systems will be removed.

When employees change jobs within the organisation/provider 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.

4.12 All users are required to manage folders appropriately and delete any unwanted items or archive them to the relevant storage.

4.13 Employees who plan to or already have an internet presence (e.g. personal blog) which indicates in any way that they work at Elmhouse Training should discuss any potential conflicts of interest with the Human Resources department. 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 Human Resources department.

4.14 Employee emails will be stored on the college mail server for 13 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.

4.15 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

4.16 Employees, temporary staff, students, governors and visitors using or administering the IT facilities must not try and prove any suspected or perceived security weakness/es.

4.17 All actual and suspected security incidents are to be reported to the Business Manager (the IT Manager 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 Elmhouse Training and/or discusses their work, they are expected to behave appropriately when on the Internet, and in ways that are consistent with the organsiation/provders values and policies.

5.2 All employees, temporary staff, students, governors and visitors who identify themselves as part of Elmhouse Training

- Must not engage in activities on the Internet which might bring Elmhouse Training into disrepute
- Must not use the Internet in any way to attack or abuse students, colleagues, teachers or tutors
- 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 Elmhouse Training , the Business Manager 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 private provider 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 the Business Manager 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 Elmhouse Training employee or do not discuss the organisation, 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 Elmhouse Training page run by the provider for Elmhouse Training 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 an Elmhouse Training brand

5.8 Wiki Sites and Online Encyclopaedia's - the Business Manager is responsible for the writing, overseeing, monitoring and updating of the providers 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 those sent by email or via the Internet. Files containing such copyright protected material should not be copied, downloaded,

forwarded or transmitted 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 provider device

6.3 All employees, temporary staff, students, governors, and visitors must not download or distribute any pirated software using the provider system. Any such action is likely to be considered as a potential act of gross misconduct and the providers Disciplinary Procedure will apply.

7.0 Data Protection and sharing information electronically

7.1 No provider/organisation data should be shared electronically with any third party without the prior permission of the Centre Manager . If agreement is in place, the information must be encrypted.

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

7.3 Please refer to the '*Data Protection Policy'* for full details.

Removable Media & Encryption

1. 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
2. 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 provider procedure available on Moodle.
3. provider owned removable media must be formatted or destroyed by the IT Support team only.
4. 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 provider procedure
5. 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
6. Report any incidents to the DPO including the loss or compromise of a device so appropriate action can be taken

Mobile working/Remote Access

1. Information should only be stored on provider systems or if remote working is required, remote access or drobox should be used
2. Devices should not be logged-on and unlocked when unattended.
3. Users shall ensure that unauthorised persons (friends, family, associates, etc.) do not gain access to mobile systems, devices or information in their charge.
4. 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.
5. 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 provider will take all necessary and reasonable steps to ensure the provider network is safe and secure. Every effort will be made to keep security software up to date. The provider hasappropriate

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 provider systems and information.

9.0 Use of images, captures or videos

9.1 The use of images, captures or videos should be encouraged where there is no breach of copyright 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. Provider owned devices should be used at all times.

10.0 Education and Training

10.1 With the current nature of internet access, it is impossible for the provider to eliminate all risks for employees, temporary staff, students, governors and visitors. It is our view therefore that the provider 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 Issues associated with e-safety apply across the curriculum and support areas and employees, temporary staff, students, governors and visitors receive guidance on what precautions and safeguards are appropriate when making use of the internet and technologies.

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 provider Equipment Signed out on Loan

11.1 All employees, temporary staff, students, governors and visitors utilising loaned IT equipment which is the property of Elmhouse Training, should be aware it should only to be used in conjunction with college business and is also covered by this acceptable usage 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 business manager on the agreed return date or the end of their contract (whichever is earliest). The equipment must be returned in the same condition as when it was issued.

11.3 The business manager hold records on college equipment loaned to employees, temporary staff, students, governors and visitors.

11.4 The following terms form part of the loan agreement between the provider and employees, temporary staff, students, governors and visitors assigned provider equipment such as a tablet, phone or other device:

- *When the item on loan is a tablet or phone, if the item is damaged whilst in my control, I understand and accept that my line manager will discuss the circumstances with me and make a recommendation to the Business Manager (which will be reviewed by a senior member of staff) if the cost of the damage incurred should be covered by the college or that I am personally responsible for the cost of a repair, replacement iPad and/or charger. Please note these are recommendations only and a final decision will be made by a senior member of staff.*

- *When the item on loan is a tablet or phone, If the item is lost whilst in my control, I understand and accept that I will be personally responsible for the cost of a replacement iPad and/or charger. If the item is lost or stolen, you must inform the Business Manager so a block can be placed on the device.*
- *When the item on loan is a tablet or phone and you are off sick, the device should not be used by anyone else. The Head of Department is responsible for making sure the tablet or phone is not in use and if they wish to reassign if to another member of staff they bring that request to IT Support - this is so the device can be wiped and signed out again, enabling IT Support & HR records to be kept up to date*
- *When the item on loan is a tablet or phone and you are on maternity/paternity leave, IT Support can keep the device safe until your return unless the Head of Department wishes to reassign to another member of staff.*
- *When the item on loan is a tablet or phone, you are required to protect it with a secure passcode that is alphanumeric & at least 6 characters*
- *When the item on loan is a tablet or phone, it is specified on the sign out form if the loan is signed out for individual use, use by anyone else is breach of policy/code of conduct*

12.0 Linked Documentation

- Password Policy
- Data Protection Policy
- Safeguarding and PREVENT Policies

13.0 Disciplinary Procedures

For members of staff who are alleged to have committed an act or acts of misconduct under this policy, the providers Disciplinary Procedure is likely to be invoked. Depending on the perceived level of alleged misconduct, disciplinary action could warrant a disciplinary sanction up to and including summary dismissal. If a breach of statutory legislation occurs, there may also be legal action instigated.

14.0 Review

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