Distance Learning and Cyber Security Policy

October 2024

Version History

Date Changed	Version	Reason	Completed By	Comments
01/10/2024	1.0	Document Creation	Michael White	Initial document created

Table of Contents

1. Introduction

Semester Learning and Development (Semester) recognises the benefits and opportunities which new and innovative technologies offer to teaching and learning. Our approach is to implement safeguards and to support staff, learners, employers and apprentices to identify and manage risks associated with distance learning and cyber security. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our associated policies.

To ensure we safeguard our staff, learners and apprentices, we will implement measures and training to raise awareness and support safety when using online systems.

This policy should be read in conjunction with other relevant Semester policies and procedures, including:

- **SEM-P001 –** Equality, Diversity and Inclusion Policy
- **SEM-P006 –** Data Protection Policy
- **SEM-P008 –** Safeguarding Policy (Keeping Apprentices Safe)
- **SEM-P009 –** Apprentice/Learner Code of Conduct
- **SEM-P012 –** I.T. Policy
- **SEM-P016 –** Complaints and Appeals Policy
- **SEM-P017 –** Whistle Blowing Policy

2. Scope

This policy applies to all employees, learners, employers and apprentices who have access to Semester's IT systems, either on premises or remotely. Any user of Semester's IT systems must adhere to this policy and the policies listed in the introduction section above.

For the avoidance of doubt, this policy applies to all uses of the internet, including web browsing, email, electronic communication and access to software provided by Semester. It also includes all internet enabled devices, such as mobile phones, tablets, smart watches, games consoles, computers and laptops.

All users are responsible for seeing that these technologies are used lawfully, ethically and courteously.

3. Objective

Semester's objective is to:

- Ensure user behaviour is safe and appropriate
- Ensure safeguards on Semester's IT based systems are strong and reliable
- Educate staff, learners, employers and apprentices on eSafety
- Ensure all incidents which threaten eSafety are managed appropriately and effectively
- Ensure a safe learning environment for all learners and apprentices

4. Definitions

Acceptable use means:

- Information/data and systems may only be used for the purpose they were designed and must not be used as a means to bully, intimidate or blackmail any person and must not be used to for unlawful content, contact or commerce

Devices means:

- Any internet enabled device, including computers, laptops, mobile phones, tablets, smart watches and games consoles

Incident means:

- Any incident that occurs and involves any person (staff, learner, employer or apprentice) where the use of technology enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of Semester. This may include the use of social media, forums, blogs, messages, digital images or any other means

Information Technology (IT) means:

- The technology that helps to produce, manipulate, store, communicate and/or disseminate information

Sensitive data means:

- Information not classified as public, must be protected and must not be disclosed i.e. personal information

Software means:

- Programs such as Microsoft products, the internet, eLearning platforms, ePortfolio platforms and video calling software

Unlawful content means:

- Exposure to illegal material, such as images of child abuse
- Exposure to age-inappropriate material
- Exposure to socially unacceptable material, such as that inciting hate, extremism, violence or intolerance
- Exposure to inaccurate or misleading information
- Illegal downloading of copyrighted materials, such as images, videos and music

Unlawful contact means:

- Bullying via any web or communication enabled device
- Grooming using any communication technologies
- Radicalisation and extreme ideologies using communication technologies

Unlawful commerce means:

- Exposure of minors to inappropriate commercial advertising
- Commercial and financial scams
- Exposure to online gambling services

User means:

- Any person authorised to use the Semester IT systems including staff, candidates and visitors

5. Online Behaviour

Semester considers it unacceptable to download or transmit any material which might reasonably be considered:

- Abusive
- Sexist
- Obscene
- Racist
- Defamatory
- Related to violent extremism or terrorism
- Intended to harass, annoy or intimidate another person

Semester expects all users of I.T. systems and devices to:

- Take responsibility for any content posted online
- Adhere to standards of behaviour and guidelines set out in the I.T. policy
- Be aware of cyber bullying, grooming law and child protection issues and forward any concerns to the Designated Safeguarding Officer
- Keep personal and professional lives separate online
- Be diligent if sharing personal details online
- Understand they are legally liable for anything they post online
- Adhere to Semester's Equality, Diversity and Inclusion policy
- Adhere to Semester's Safeguarding policy (Keeping Apprentices Safe)

Semester will take appropriate action, which may include notifying the police, in the following circumstances:

- Any online conduct considered to be illegal
- Any instances of bullying or abuse online
- Any online comments which could bring Semester into disrepute or cause reputational damage
- Any comments made online which could be reasonably considered to be abusive, sexist, obscene, racist, harassing, intimidating, defamatory or which relate to violent extremism or terrorism

6. Online Safety

Staff should continue to develop learners'/apprentices' knowledge on how to keep themselves safe online and seek opportunities to remind them of this during reviews and tutorial sessions.

It is imperative that all staff who interact with young and vulnerable people online continue to look out for signs a young/vulnerable person may be at risk. Any such concerns should be dealt with in line with the Semester Safeguarding Policy (Keeping Apprentices Safe) and where appropriate referrals should be made to local safeguarding contacts or the police, as required.

Semester will ensure that any use of online learning tools and systems are in-line with privacy and data protection/GDPR requirements.

7. Interactive Platforms

Semester utilises the following interactive platforms to support a blended learning model. All of these platforms require the use of a device with internet connectivity:

OneFile – Learners and apprentices can utilise OneFile to monitor their progress, record evidence against their learning aims and learn in a way which suits them. Employers can use OneFile to monitor their apprentice's progress, communicate with Semester and contribute to review meetings. Assessors and tutors can use OneFile to monitor progression, communicate with learners, apprentices and employers and allocate tasks, actions and assignments.

Microsoft Teams/Zoom – Apprentices and assessors utilise these platforms for 1-1/group teaching, learning and assessment activities, 1-1 coaching sessions and reviews.

BKSB – All learners and apprentices have a personal account providing access to initial assessment, diagnostics and an individual learning plan (ILP) for maths, English and IT as appropriate. Interactive resources enable learners/apprentices to learn at a suitable pace through their ILP and skills checks enable tutors to monitor the progress that learners and apprentices are making these curriculum areas.

Semester Moodle platform – Semester's eLearning platform (Moodle) provides learners and apprentices with access to a range of eLearning courses and modules to enhance their knowledge and understanding in their chosen vocational pathway.

8. Online Security

When learners and apprentices use personal devices to access Semester interactive platforms, they are reminded of the security risk to data. Although they only have access to their own personal data when using these platforms, we recommend they take additional steps to protect this data and protect themselves from cyber threats. These recommendations include:

- Keep all devices password protected
- Install antivirus software and keep it up to date
- Ensure you do not leave your device(s) exposed or unattended
- Install security updates and patches for browsers and systems as soon as they are made available

Employees should avoid accessing internal systems and accounts from other people's devices or by using public wireless networks. Employees must not make their devices available to others, unless authorised to do so by a Senior Manager.

8a. **Emails**

Email messages are often used to propagate scams and malicious software (e.g. Malware and links to malicious software hosted on the internet). This presents a risk of users being tricked into giving up their usernames and passwords, or other personal information. This type of trickery is known as phishing or whalling attacks and the messages often contain links and attachments, which prior to clicking on or opening, look convincing. To avoid the risk of virus infection or data theft, we recommend you:

- Avoid opening attachments when the content is not adequately explained – for example, 'watch this video to see more'
- Avoid clicking on links embedded within emails unless you trust the source
- Be suspicious of clickbait – for example, emails offering prizes
- Look for inconsistencies in the email content – for example, grammar mistakes, incorrect use of capital letters, spelling mistakes or excessive use of exclamation marks
- Check the name and the email address of the person you received the message from – do you recognise the name and the email address, and does it look legitimate?

8b. **Passwords**

When creating a password, please consider the following:

- Passwords should be at least 8 characters long and should include capital and lower-case letters, numbers and symbols
- When asked to change a password, don't use the same password again or a password you have used recently
- Avoid picking easily identifiable words or phrases – for example football teams, children's names or birthdays
- Avoid using the same password for multiple website and systems
- Create a password you can remember and do not write it down anywhere

8c. **Data Transfer**

Transferring data can introduce a serious and significant security risk. Users must:

- Avoid emailing sensitive data as an attachment
- Avoid transferring sensitive data to other devices or accounts
- Avoid sharing confidential data using a public Wi-Fi network
- Use encryption tools to protect sensitive or confidential data
- Ensure the recipient of the data is properly authorised to receive it
- Report any scams, hacking attempts or privacy breaches

8d. **Additional Measures**

To reduce the likelihood of security breaches, we also recommend users to:

- Turn off their screen and lock their device when leaving it unattended
- Avoid accessing suspicious websites
- Refrain from downloading or installing suspicious or illegal software
- Install or activate firewalls and anti-malware software
- Change all account passwords at once if a device is stolen
- Report any perceived threat or possible security weakness immediately to a senior manager

9. Online Code of Conduct

Currently, all of Semester's delivery, assessment (except end-point assessment), one-to-ones and review meetings are carried out remotely, using various technology solutions.

Where staff are delivering training, reviews or attending Teams/Zoom meetings, they must ensure that the environment is appropriate (not a bedroom or a public location), free from interruptions (children, pets etc.) and free from external noise and distractions.

Learners and apprentices attending reviews, one-to-ones or live training sessions from home should ensure that they are in an appropriate environment (not a bedroom) which is free from distractions and background noise.

Staff, learners and apprentices must wear suitable clothing during any review, one-to-one or live training session. They should also ensure that anybody else in the household, who could make an appearance at any stage on camera, is wearing suitable clothing. Computers should be in a suitable location and no personal items or photographs should be in view. It is also recommended that when using Microsoft Teams or Zoom, that the background is blurred.

Staff are only permitted to use online platforms which have been specified by their manager and approved by the Operations Manager or Services Director. Staff should record the date, time and length of any online session, in addition to capturing attendance and any relevant notes. Staff must also record any disruptions, issues or concerns during an online session which may be useful in the event of a complaint or appeal.

When communicating with learners, employers or apprentices, staff must only use their work email address or a phone (or phone number) provided to them by Semester.

Language during any online session must always be professional and appropriate. This includes any family member or other people in the background. This applies to staff, learners, employers and apprentices.

During online reviews, live training sessions and one-to-ones, staff, learners and apprentices should have their camera switched on and their microphone active. The host should take control of the session and should inform the learner/apprentice if they want them to mute their microphone or switch off their camera.

For learners/apprentices to be able to progress to the next stage of achieving their career goal or their next step in their chosen programme, it is vital that they participate and engage in any review, one-to-one or training session. Learners/apprentices may risk their place on their course if they fail to attend or participate in their learning activities.

10. Cyber Essentials

Semester is currently certified for Cyber Essentials. This is a government backed scheme that helps organisations protect themselves against the growing threat of cyber-attacks. The certification provides a clear statement of the basic controls Semester has in place.

11. Disciplinary Action

We expect all users to maintain an awareness of the importance of cyber security. It is an expectation that all users of Semester systems and interactive platforms follow this policy, and any associated policy (as listed in the introduction section). Users who are observed disregarding this policy may face disciplinary action, even if their disregard has not resulted in any security breach. Users who cause security breaches may face disciplinary action as follows:

- **First-time, small scale or an unintentional breach:** A verbal reminder of security importance and possible requirement to attend refresher cyber-security training
- **Intentional, repeated or large-scale breaches (those which cause loss of service, financial impact or other damage):** These instances could lead to significant disciplinary action (for staff) or termination from their training programme (for learners and apprentices)

12. Review and Monitoring

This policy will be monitored annually as part of Semester's internal review process and will be reviewed on a three-year cycle, or as required by legislation changes.