E-Safety & Acceptable Use Policy

Table of Contents

Introduction

Pentagon Skills recognises the benefits and opportunities which new technologies offer to our business, teaching, learning and assessments. We operate a number of cloud based and online systems to aid both the operation of the business and to provide staff and learners with tools and resources that aid in the effective delivery of our training and qualifications however, the accessibility and global nature of the internet and different technologies used to access it mean that we are also aware of potential risks and challenges associated with such use.

Our approach is to implement appropriate safeguards within our systems and devices, while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care.

Definitions

Device(s)	Refers to all computer equipment including laptop, desktop, mobile phone, tablet and any other asset owned by Pentagon Skills Ltd
System(s)	Refers to all software, learning tools, e-portfolios, social media accounts and digital solutions that are employed within the running of the business for any purpose.

Scope of the policy

This policy applies to all staff, learners and others who have access to Pentagon Skills devices or systems both on company premises and via remote access. Any user of Pentagon Skills devices or services must adhere to this policy as it applies to all use of the internet and electronic communication devices and services such as e-mail, mobile devices, social networking sites, e-portfolio, online training platforms and any other systems that use the internet for connection, data processing and other related activity.

Responsibilities

Pentagon Skills Ltd has a responsibility to:

- Ensure Pentagon Skills systems and devices are fit for purpose
- Ensure Pentagon Skills systems and devices are used responsibly and safely by learners and staff
- Ensure that the risk of data breach or cyber-attack is minimised through the implementation of robust security measures that are reviewed and communicated to staff and learners
- Set out policies and procedures that ensure the objectives are met and set guidelines for reporting, support and training.

Pentagon Skills Managers are responsible for: -

- Operating in line with the policies and procedures set out by the business
- Seek advice and support from specialist contractors or colleagues to ensure compliance (where needed)
- Ensuring that their staff are aware of this policy and procedure and how it operates
- Ensuring that relevant checks are carried out as required in line with the policies and procedures
- Ensuring that the policy is communicated and accessible to those who require it
- Immediately reporting any breaches or suspected breaches of any of the policies and procedures set out by Pentagon Skills Ltd.

Individual members of staff have a responsibility to: -

- Be aware of this policy and procedure and ensure that they comply with its requirements
- Seek advice and support from line managers to ensure compliance (where needed)
- Immediately report any breaches or suspected breaches of any of the policies and procedures set out by Pentagon Skills Ltd.
- Immediately report any cyber attack/ suspected cyber attack, data breach/ suspected data breach or any suspicious occurrences to their line manager

Individual learners have a responsibility to:

- Use Pentagon Skills services and devices in a responsible and safe manner within the confines of the policies and procedures.
- Immediately report any cyber attack/ suspected cyber attack, data breach/ suspected data breach or any suspicious occurrences to their assessor, tutor or line manager

Technologies

The technologies covered by this policy are computer, Internet, electronic communication and mobile devices such as mobile/smart phones and PDAs.

Current Internet technologies used both inside and outside of the classroom include:

- Websites
- Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking

Students may be working online in classrooms, at home or elsewhere. They may be using personal devices not covered by Pentagon Skills security systems and everyone to needs to understand the risks and act accordingly.

Stakeholders

This means that designing and implementing e-safety policies demands the involvement of a wide range of interest groups: -

- Senior Managers.
- Teachers and Support Staff.
- All learners, particularly young people and vulnerable adults.

Pentagon Skills has implemented systems to minimise the risk of cyber-attacks or data breaches by implementing:

- industry-leading endpoint EDR protection and system health monitoring software to detect and respond to potential threats promptly.
- Firewalls, to stop unwanted intrusion from external locations and ensure that students/staff cannot access external websites without using the Internet content filtering system.
- Virus protection checks all files, emails, websites for virus and cleans/quarantines the virus as appropriate.
- Network security, using usernames and complex passwords.
- Setting user access limitations ensuring that staff and students can only access their own files, accounts or designated shared access areas.

Monitoring

Pentagon Skills monitor access to all IT systems, this includes the logging on/off computers systems, internet activity, virtual learning environment (Quals Direct), and e-mails. Monitoring will only be used to confirm or investigate compliance with other policies and procedures.

Internet Use

It is impossible to be completely protected while using the internet. However, the following policies should ensure that risks of a cyber-attack or data breach are minimized:

Password Creation

Creating strong, effective passwords is the first step in protecting our systems. To create a robust password, one should combine uppercase and lowercase letters, numbers, and special characters. Avoid easily guessable information such as names, birthdays, or common words. Passwords should be at least 12 characters long. Changing passwords is also a good practice to enhance security although current guidance suggests that complex passwords that have been formed as per Pentagon Skills Ltd Password Policy should remain fit for purpose for 12 months unless a data a leak or any attacks are attempted.

ACTION - It is your responsibility to ensure all passwords are formed in line with ‘Pentagon Skills Passwords Policy 2024’.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security measure that requires more than one method of authentication to verify a user's identity. This is important because it adds an extra layer of protection to accounts. Even if a password is compromised, the attacker would still need to bypass additional verification steps, such as a code sent to a mobile phone. Implementing MFA significantly reduces the risk of unauthorized access because even if someone has your log in details you will need to agree with the access request or provide a code to the hacker/ scammer in order for them to log in.

ACTION - It is your responsibility to ensure that Multi-Factor Authentication (MFA) is set up and working on all accounts that include this feature and report immediately to your line manager if you experience any technical difficulties.

Exercising Caution

Safe use of the internet involves being cautious and vigilant while browsing. The use of Pentagon Skills Ltd devices is limited to activity required for work only, no gaming, personal shopping or browsing of untrusted website is permitted. Users should only visit trusted websites and avoid clicking on unknown links or downloading suspicious files. It is crucial to keep browsers and security software updated to defend against the latest threats. Do not share login, password or personal information with anyone or on public forums or unsecured websites. Using a Virtual Private Network (VPN) can add an extra layer of security when accessing the internet from public Wi-Fi networks.

ACTION – Check for the padlock on the website URL. Only use your work devices for work purposes and never share the password to your work device with anyone else. Do not allow others to use your work device for any reason.

Phishing Emails

Phishing emails are very dangerous fraudulent emails that appear to be from legitimate sources to trick recipients into revealing personal information or installing malware. Great care must be taken when reading and opening emails to ensure that our systems remain secure and free of malware. To detect phishing emails you should follow the process below:

- Check the email address! This is the first and most important step in reading any email. The name might display as the business name the email is supposedly sent from but when you click of the email address it will be irrelevant code or a long complicated address with the business name inside. If in doubt do nothing with the email and REPORT IT!
- Look for signs such as generic greetings (Hi, Hello Dear, Good Afternoon etc)
- Check spelling and grammar many are badly written with poor spelling and have code remaining in the email.
- Unexpected attachments or links. Never click a link or download an attachment until you are certain who the email has come from. If in doubt do nothing with the email and REPORT IT!

ACTION – Be vigilant when checking and responding to emails. Thoroughly check for the points above and if in doubt do nothing and report it. Where it is obvious that an email is a Phishing email then it can be deleted and reported.

Phishing Text Messages

Phishing text messages, also known as smishing, are deceptive messages sent to trick users. One common scam is the 'mum scam,' where the attacker pretends to be a family member in distress to solicit emergency funds. Other scams include fake bank alerts, fake texts about attempted deliveries of parcels and too-good-to-be-true offers. Always verify the sender's identity before responding to

unexpected text messages. Contact the person or organization directly using official contact information on their official website if in doubt.

ACTION – Be vigilant when checking and responding to texts. If in doubt contact the business directly and report it to your line manager.

Phishing via Social Media Messages and Adverts

Phishing can also occur through social media messages and adverts. Attackers may create fake profiles or advertisements to lure users into providing sensitive information or clicking on malicious links. To identify phishing attempts on social media, look at the persons profile to check how many friends they have and how long the account has been active. In many cases you will find generic information with no or few photos of the person they are claiming to be. Look at the quality and professionalism within messages, requests for personal information, and high-pressure tactics, if something does not seem legit then it probably isn't. Check if the item they are trying to buy or sell seems to be the right price and never accept payment before collection, there are a number of scams associated with accepting payment online before someone arrives to pick the item up and they result in you losing money.

ACTION - Avoid clicking on unknown links or accepting friend requests from unfamiliar profiles. Report suspicious activity to the social media platform and your line manager.

Search Engines

Search engines enable the rapid search of the internet for information, whether this information be text, image or sound. Searching consists of entering a word or words into a search box and clicking the search button, which sets in motion a search engine that automatically produces a list of the addresses of websites relevant to the words entered. Many search providers also offer the facility for the user to search for images, video and audio content.

The more accurate your search is (i.e. using more than one relevant word), the more relevant the search results will be and thus the less likely that unwanted results will be prominently returned. For example, if you are searching for information on the planet Mercury, entering 'planet mercury' into the search box will get more relevant results than just entering 'Mercury'.

Take care to spell correctly when typing in a search. Even a small typing error can bring up unwanted results. Remember that not all the information in websites returned in searches is reliable and some websites presented could be that of a scammer.

There are two types of search results:

- Automated search results
- Sponsored listings.

Search providers usually separate and label these but it is important that you are aware of the difference and can differentiate them in the results of the search provider you are using. Whichever search provider you choose, it is important that you familiarise yourself with this

provider's service, finding out about the search provider's safety advice, the search provider's filter, how to contact the search provider, and how sponsored listings are differentiated from other search results.

Social Networking Sites

Social networking sites (like Facebook) are online 'communities' of internet users with similar interests. Members of the community create an online 'profile' which provides other users with varying amounts of personal information. Once users have joined the network, they can communicate with each other and share things like music, photos and films. The sites are a fun way to stay connected with friends, family and peers.

As with most potential online dangers, the problems can start if you do not look after personal information properly. The risks you need to be aware of are:

- Cyberbullying (bullying using digital technology).
- Invasion of privacy.
- Identity theft.
- Seeing offensive images and messages.
- The presence of strangers who may be there to 'groom' other members.

Staying Safe Using Social Networking Websites

- Don't publish personal information like location, email address, phone number or date of birth.
- Be very careful about what images and messages are posted, even among trusted friends – once they are online, they can be shared widely and are extremely difficult to get removed.
- keep a record of anything abusive or offensive received and report any trouble to the site management (most sites have a simple reporting procedure, normally activated by clicking on a link on the page).
- Be aware that publishing or sharing anything which would mean breaking a copyright agreement is illegal.
- If you make an online friend and want to meet up with them in real life, ensure you have a responsible adult with you to check the person is who they say they are.
- Be aware of online scams – offers which seem too good to be true usually are.
- Do not to get into any online discussions about sex as this tends to attract potentially dangerous users.

E-Mail

- Do not forward chain letters to anyone else, consider the information being transmitted and review the email trail before each email transmisision.
- Do not impersonate anyone else using e-mail.
- Do not use e-mail to send comments or information that is defamatory or libellous, or use e-mail as a means of harassment, intimidation, annoyance or bullying to anyone else. The

sender of an e-mail should only send messages the contents of which they would be happy to receive or have read out in court. E-mail messages are admissible as evidence.
- Do not reply to pestering, offensive or suggestive e-mails, students should report such occurrences to their line manager, assessor or trainer.
- The biggest cause of computer viruses is sent by email, often innocently. If you think you have received a virus, or are suspicious about an email received, delete the email without opening it and report it.

Reports, Concerns & Complaints

All queries and concerns should be addressed to Pentagon Skills Operation Manager Scott Hamer in the first instance. Proven incidents of internet misuse or other breaches in acceptable use will be taken very seriously and may be dealt with through college procedures relating to conduct, harassment or bullying.

Concerns relating to safeguarding, including child protection must be referred immediately to the designated person responsible for safeguarding/child protection.

Points of contact

Mr Scott Hamer
Tel: 07904215965
Email: scott@pentagonskills.co.uk