CONSTRUCTION & PLANT ASSESSMENTS
The Flooring Academy

E-Safety Policy & Procedure

Introduction

Construction and Plant Assessments (CPA) recognises that technology and the use of ICT equipment is part of everyday life and that it is an essential part of learning and employment.

ICT systems are one of the fastest and most effective ways of finding information, sharing ideas, and working with other people but, while effective, there is also the opportunity for risks to occur. As part of our safeguarding responsibility, we aim to protect all staff and learners against risks associated to the internet and other technology aids such as mobile phones. This will be known as e-safety.

The risks to users can include data that is inaccurate, dangerous, illegal, and offensive.

Risks

The risks associated with technology can be categorised under the following headings:

Physical: Including poor posture, affected by poor seating and furniture set-up, and eye strain due to the length of time a person is exposed to the screen.

Contact: Social networking sites and chat rooms allow you to meet new friends but unfortunately not everyone is who they claim to be. Never give personal information out as this could make you vulnerable to exploitation, bullying or sexual aggression.

Conduct: This behaviour can be by, or towards, individuals and can include cyberbullying and cyberstalking. Behaviours can also include racism and piracy. When using equipment provided by CPA and your employer, you have a right to be protected and a duty to behave honestly and responsibly. Never do anything that makes you vulnerable to malicious software or charges of bad behaviour. Incorrect use of equipment, including downloading or passing on illegal or inappropriate content, can result in the user committing a criminal offence.

Content: This includes downloading information, some of which may be illegal, dishonest, or inappropriate. This presents risks to the learner/staff member and your employer/ training provider if using their equipment. Posting personal information can also pose risks as previously mentioned in the "contact" category.

Commerce: This includes the risk of financial abuse when making a purchase online through an unsecure source. Always check that a site belongs to the company it says it does – if in doubt, look for a real-world postal address or phone number.

Our aim

In order to safeguard our staff and learners against the risks associated to using the internet and other technology aids, CPA aims to:

- Provide all staff and learners with sufficient information regarding the risk's technology can present and help them develop the skills to safeguard themselves. This will act in accordance with our Safeguarding Policy, Health and Safety Policy, Equality and Diversity Policy and Whistle-blowing Policy.

- Work together with outside agencies to develop a consistent coherent approach to safeguarding.
- Involve managers, staff, learners and employers in the development and review of policies and procedures for safeguarding and unacceptable use of technology.
- Have an appointed Safeguarding representative who will deal with all safeguarding issues.
- Provide ongoing review and assessment with learners to discuss learning and development needs and address any Health and Safety, Equality and Diversity and Safeguarding concerns.
- Provide all staff with appropriate safeguarding training that includes the safe use of technology.

Responsibility

Our Safeguarding, Health and Safety, Equality and Diversity policies and procedures demonstrate our responsibilities and duty of care in protecting all our staff and learners from harm, including potential harm from the internet, social networks, and other electronic media.

CPA has appointed a Lead Designated Safeguarding Officer who is responsible for ensuring that policies are implemented, and that regular monitoring takes place. All learners and staff should be made aware of safeguarding policies. All users should be encouraged to use computers and the internet responsibly and to understand the consequences their actions could have on themselves and others. This will also include the safe use of mobile phones and social media sites.

Lead Designated Safeguarding Officer

The Curriculum Manager (David Russell) has been appointed as the Lead Designated Safeguarding Officer, with support from Lindsey Russell, Deputy Safeguarding Officer and are responsible for ensuring:

- This policy is issued to all members of staff.
- Learners, employers, and sub-contractors are aware of this policy.
- Where necessary, inform parents and carers of this policy.
- The regular review of this policy, taking into account changes in technology.
- Guidance and training is provided to all staff with a responsibility for the delivery or invigilation of internet-based learning.
- Staff understand the contents of the materials provided to support the safe use of the internet and copyright legislation.
- Existing policies and codes of practice in relation to safeguarding reflect the threat of technology abuse.

Tutors and Assessors have the following responsibilities:

- Provide information about learner safety and security related to the internet and electronic communications to all learners at induction and throughout the learner journey.
- Ensure that all internet access is supervised.
- Ensure learners and all other non-employees of CPA are not given passwords and access to staff and management information systems
- Ensure that that the WI-FI password is not given out to Learners.
- To connect to the internet only through the filtered network service.
- To ensure staff and learners are aware that their internet activity is monitored by CPA.
- To reinforce the understanding of learners that material on the internet is also subject to copyright legislation and to reinforce that plagiarism of material from the internet is not acceptable unless referenced within the main text or bibliography.

All Employees of CPA Must:

- Never hold in their possession illegal materials/images in electronic or other format.
- Never download or access illegal images or sites at any time or in any place through CPA facilities both on and away from CPA premises.
- Ensure they are fully aware of this and other related policies and ICT guidelines and adhere to them.
- Ensure all communication with learners is solely for the purpose of learning, teaching and assessment and carried out in a professional manner using only an official CPA email address and telephone/mobile phone number.
- Never engage with any learners via contact/webcam sites (for example chat rooms, message boards and newsgroups) for any purpose other than teaching and learning and always record the content of this delivery method and purpose for its use.
- Never engage in communication with individuals under 18, or who are deemed to be vulnerable, using this via contact/webcam sites (for example chat rooms, message boards and newsgroups) for any purpose.

Responsibilities of Learners

- To have a responsible attitude to the use of ICT equipment and internet/email provision.
- To agree to and follow policies and guidelines on acceptable use and to report any misuse or suspected misuse by others, including bullying and harassment via electronic means.
- To follow the Internet Safety Rules.
- Learners should not use USB or other devices without the permission of a CPA member of staff on any CPA laptops to avoid the transfer of viruses and unsuitable material.
- Learners must ensure these devices are free of viruses before use.

Guidance to Learners

CPA staff should give information to learners on internet safety which includes:

- Ensuring they never tell anyone they meet on the internet, personal details such as their home address, phone numbers, photos, or bank details.
- Ensuring they never tell anyone they meet on the internet their employer's name or phone number.
- Never arranging to meet in person someone they first met online.
- Ensuring they understand that not everything they read online is true.

Guidance to Visitors

On the rare occasions where visitors have access to our internet and ICT systems, the same responsibilities for learners apply. Visitors must obtain authorisation to have access to the internet and internal ICT systems but must not be given access to the staff intranet unless there is a legitimate reason.

Supervision of Learners

Training and Assessments Officers and Invigilators have a responsibility to maintain the safety of learners when using ICT equipment. The following guidance should be adhered to when supervising learners:

- Learners should never be left unsupervised when using the internet.
- Computers should be within sight of the tutor and assessor and for examination purposes, the invigilator.
- Employers who have learners on work placement should be informed of this policy and should not allow them to have unsupervised unfiltered internet access.
- Rules outlining the use and restrictions when using the internet should be available to all learners if they have access to the internet.

Use of the Internet

The following internet procedures must be followed by all users to ensure safe and responsible use of the internet. It should always be remembered that all internet usage is recorded and can be traced back to the user.

- Staff should inform the Director and learners should inform their Tutor/Assessor or Employer immediately if any abusive, threatening, or offensive sites are discovered.
- Care should be taken that any material published to the web does not breach any of the guidelines in this policy or other policies relating to data protection, copyright, and Intellectual Property Rights (IPR).
- Personal information should never be disclosed to others.

Use of Email

The following procedures must be followed by all users, including staff, to ensure safe and responsible use of email. It should be remembered that emails are recorded, can be traced back to the sender and can be legally binding.

- Users should change passwords regularly and should not share them with others.
- Learners should inform their tutor/assessor or employer immediately if any abusive, threatening or offensive emails are received.
- Inform their tutor/assessor or employer immediately if an email or attachment generates a virus warning.
- Staff should be aware that their email is filtered, and no organisational email accounts are private.

The contents of staff e-mail accounts or details of online activity may be checked at any time.

- Staff should never use CPA internet and email accounts to send private confidential information or provide credit card details.
- Staff should be aware that their email use and internet activity is monitored and recorded.

Staff working with young people should ensure that:

- They do not engage in private/personal communication with a learner. This includes texting and media messaging, e.g., MSN Messenger, and social networks, e.g., Facebook, Skype etc
- They take care in communicating with learners via email and ensure it is for training and assessment purposes only. Staff must ensure their communication is non-discriminatory or offensive.

Virus Protection

All CPA equipment used for access to the internet is installed with anti-virus software.
Introducing viruses to computers, or attempting to break through network security, is a serious offence and users should be aware of the issues and the risks.
Any learner who suspects the presence of a computer virus must alert their Tutor/Assessor.

Copyright

Copyright rules apply to material available over the internet and will generally be subject to the same level of protection as material in other media. Although there are no specific exceptions from copyright material on the internet, those relating to fair dealing for the purposes of non-commercial research or private study may apply.
Users should be aware of copyright notices on websites setting out how the material may be used and how to obtain permission.

Guidelines on the use of material off the internet are as follows.

- Learners and staff should acknowledge any sources within any documentation they have produced.
- Users should not assume that educational use of material is permitted, without first checking with the author. Web-based resources may themselves have been published without the appropriate permissions. Therefore, any subsequent use of such material may also be illegal.
- Publishing other people's material without their explicit permission is a breach of copyright. This applies to the use of images from the internet used within a document.
- Showing and accessing websites in a lesson is not a breach of copyright but copying an entire page without appropriate permission for own use, *e.g.,* a PowerPoint presentation, is.
- Copying material from the internet and printing it for pupil use could be a breach of copyright. Using it as part of a larger document without appropriate permission would be a breach of copyright
- Copyright laws vary between countries.

Website Development

- Access to CPA's website is open to all. However, the authority to be able to add information to the website is restricted to designated staff and monitored by the Director.
- Where a picture or image of a learner, employer and or a member of staff is used, permission to use this image will be sought from the individual beforehand. Where a learner is aged below 18, consent will be gained from parents/carer.
- CPA is aware that images can be downloaded from the internet, including websites by others, without the authority or permission to do so.
- CPA has a responsibility to protect all staff and learners in their care and will consider the risks involved in any information which appears on our website.

Our commitment to ensuring a person's rights and safety are not violated include:

- Ensuring names and photographs of learners, staff and individuals deemed vulnerable should not appear on our website.
- Photographs of groups of young people may be posted but only with written parental permission for all members of the group.

- Ensuring parents/carers of learners and staff under the age of 18 are fully informed of these procedures and the reasoning behind them

Mobile Phones and Electronic Devices

In order to protect individuals from personal safety issues that may occur, CPA does not ban the use of mobile phones by learners and expects all staff who are issued mobile phones by the company to carry them for their own safety.

However, the following rules should be followed to minimise the risk of inappropriate or illegal use of these devices while learners are undertaking training and assessment with CPA:

- Learners' mobile phones must be completely switched or set to silent off during all training and assessment sessions unless special permission is given by the appointed tutor/assessor.
- Inappropriate use of text messaging is not allowed at any time by staff and learners.
- Digital video or still cameras should never be taken into health and social care or childcare establishments at any time in order to protect the client group.
- No photographs, video or sound recordings can be taken without the approval of the subject, whether learners or staff.
- Bluetooth technology should not be used to transfer images at any time by staff or learners. Such images can be picked up by other Bluetooth enabled devices belonging to others in the area
- These rules apply to any equipment offering the same functions as mobile phones.
- Incidents of intimidation and bullying with such devices will be referred to the company's Lead Designated Safeguarding Officer. If the incident involves a staff member, they may be subject to disciplinary proceedings.
- Serious incidents of intimidation and bullying will be reported directly to the police.

Staff must not engage in the use of these technologies for their own personal use in working hours:

- Use of the internet to harass, offend or bully any other person.
- Use of the internet for any inappropriate or illegal purpose.
- Use of the internet for transmission of threatening, offensive or obscene material.
- Use of the internet for transmission of material from any criminal organisation.
- Use of the internet for the transmission of viruses or unlicensed software.

Disciplinary Procedures

CPA will not tolerate any behaviour that places staff and learners at risk. Any staff who fail to comply with this policy may be subject to disciplinary action.

Learners who fail to comply with this policy may face termination of their training programme.

Any allegations that have justifiable evidence of criminal activity will be referred directly to the police.

If a member of staff is suspended pending investigation, permissions to use CPA's ICT resources will be prohibited. Use will only be reinstated if the investigation is resolved, and the member of staff is reinstated.

This policy should be read in conjunction with the following policies:

- Safeguarding Policy (P&P 001)
- Health and Safety Policy (P&P 032)
- Equality and Diversity Policy (P&P 007)
- Data Protection Policy (P&P 009)
- Whistle-Blowing Policy (P&P 014)