E-Safety Policy

Date: May 2017 *Review Date:* 3 years: May 2020

Director's: Karen Smith and Ali Anwar

New technologies have become integral to the lives of everyone in today's society, both within work and training and in their lives outside at home.

The development and expansion of the use of ICT, and particularly of the internet, has transformed learning in recent years. Everyone will need to develop high level ICT skills, not only to maximise their potential use as a learning tool, but also to prepare themselves as lifelong learners and for future employment. The CADcentre has made a significant investment to ensure these technologies are available to all learners. Use of the internet is not without risks.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps both staff and learners, gain knowledge from each other. The CADcentre believes that staff and learners should have an entitlement to safe internet access at all times.

However, the use of these new technologies can put staff and learners at risk within and outside the CADcentre, including using their Employers devices in relation to their employment and their own personal devices when using the internet for personal use.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet for sexual, or financial exploitation, or being drawn into radicalization or extremism.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying including "trolling".
- Access to unsuitable video/ internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement, for copying other people's work
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of a child/ young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other CADcentre policies (e.g. Equality and Diversity, Health & Safety, Safeguarding , Prevent: Radicalisation & Extremism, Health & Wellbeing, and ICT acceptable Use policies).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential to build staff and learners resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope of the Policy

This policy applies to all staff, learners and visitors who have access to and are users of CADcentre ICT systems.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the CADcentre.

Directors:

Directors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Director's receiving regular information about e-safety incidents from Centre Managers.

Centre Manager's
are responsible for ensuring :

- the safety (including e-safety) of learners and staff in their centre
- that there is a system in place to allow for monitoring and support of those who carry out the internal e-safety monitoring role
- all learners who may attend the centre for workshops/ exams and staff complete an 'Acceptable Use Policy Agreement'
- that they take day to day responsibility for e-safety issues
- that all staff are aware of the procedures to be followed in the event of an e-safety incident taking place.
- training and advice for staff is provided
- reports are made to Director's regarding any incidents relating to e-safety

Centre Managers should be trained in e-safety issues and be aware of the potential for serious safeguarding issues arising from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming whether for sexual or financial exploitation, or being drawn into radicalisation and extremism
- cyber-bullying including trolling

Staff
are responsible for ensuring that:

- they have read, understood and signed the CADcentre Staff Acceptable Use Agreement
- they report any suspected misuse or problem to the Centre Manager for investigation/action/ sanction
- digital communications with learners (email / Virtual Learning Environment (VLE) / voice recordings) should be on a professional level and only carried out using official CADcentre systems
- e-safety issues are embedded in all aspects of learning activities
- learners understand and follow the CADcentre e-safety and acceptable use policy
- they monitor ICT activity
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current CADcentre policies with regard to these devices
- in training sessions/unit choices where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Any learner who attends for training or workshops in the centre's:

- are responsible for using the CADcentre ICT systems in accordance with the Learner Acceptable Use Agreement which they will be expected to sign before being given access to CADcentre ICT equipment and systems
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand CADcentre policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand CADcentre policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies.

Technical – infrastructure / equipment, and monitoring
The CADcentre will be responsible for ensuring that the network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented.

- There will be regular reviews and audits of the safety and security of CADcentre ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Any monitoring issues should be reported immediately the Centre Manager

- Staff regularly monitor the activity of users on the CADcentre ICT systems and users are made aware of this in the Acceptable Use Agreement
- Users are not allowed to use computers, laptops or portable devices for personal use, on or off CADcentre premises
- Staff are forbidden to install programmes on CADcentre workstations / portable devices, unless they have specific permission from the Centre Manager
- Staff can only use removable media (e.g. memory sticks / CDs / DVDs) on CADcentre workstations / portable devices, with prior permission from their centre manager
- Learners can only use removable media (e.g. memory sticks / CDs / DVDs) on CADcentre workstations / portable devices, with prior permission from their assessor/centre manager
- Individual workstations are protected by up to date virus software, and encryption
- Personal data cannot be sent over the internet or taken off CADcentre premises unless safely encrypted or otherwise secured
- All users are forbidden from using the CADcentre name, or any images taken whilst on CADcentre premises on the internet, social networking sites (e.g. on facebook, twitter etc)

Curriculum

E-safety should be a focus in all areas of the training programmes and qualifications and staff should reinforce e-safety messages in the use of ICT.

- in training sessions/units where internet use is pre-planned, it is best practice that learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches .
- Where learners have to freely search the internet, when conducting research, staff should be vigilant in monitoring , where possible, the content of the websites the learners visit
- With regard to the Digital Literacy ESW, learners have to research collaborative websites and social media sites to communicate with other users. All learners will have signed the Learner Acceptable Use policy and be aware of the protocol when communicating to other learners from other companies.

On-line resources .

The CADcentre has invested heavily in the e-portfolio system SMART Assessor.

All learners and staff must use this e-portfolio system according to the rules of the ICT Acceptable Use policy, and only upload their own work, and not upload any offensive, discriminatory or illegal material.

The on-line City & Guilds awarding body resource Smart Screen, is a resource site that must be used according to site rules and the ICT Acceptable Use policy.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning/training, allowing staff and learner's instant use of images that they have recorded themselves or downloaded from the internet. However, staff and learners need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

- When using digital images, staff should inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but must follow CADcentre policies concerning the sharing, distribution and publication of those images. Those images should only be taken on CADcentre equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that learners are appropriately dressed and are not participating in activities that might bring the individuals or the CADcentre into disrepute.
- Learners must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or newsletters or elsewhere that include learners will be selected carefully and will comply with good practice guidance on the use of such images including obtaining the written consent from the individual.

Data Protection & Data Security
Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. The loss of personal data is taken extremely seriously by the Information Commissioner.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be password protected
- the device must be password protected (many memory sticks / cards and other mobile devices cannot be password protected)
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

Communications
When using communication technologies the CADcentre considers the following as good practice:

- The CADcentre email service may be regarded as safe and secure and is monitored. It is encrypted by the provider. Staff should therefore use only the CADcentre email service to communicate with CADcentre related business.
- Users need to be aware that email communications will be monitored
- Users must immediately report, to their Centre Manager – the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff and employers/learners (email, chat) must be professional in tone and content. These communications may only take place on official (monitored) CADcentre systems. Personal email addresses, text messaging or public chat / social networking sites must not be used for these communications.
- Learners should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the CADcentre website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate / illegal activities
Some internet activity e.g. accessing child abuse images , distributing racist material or accessing sites which promote radicalisation and terrorism , is illegal.

Other activities e.g. Cyber-bullying could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a training context, either because of the age of the users or the nature of those activities.

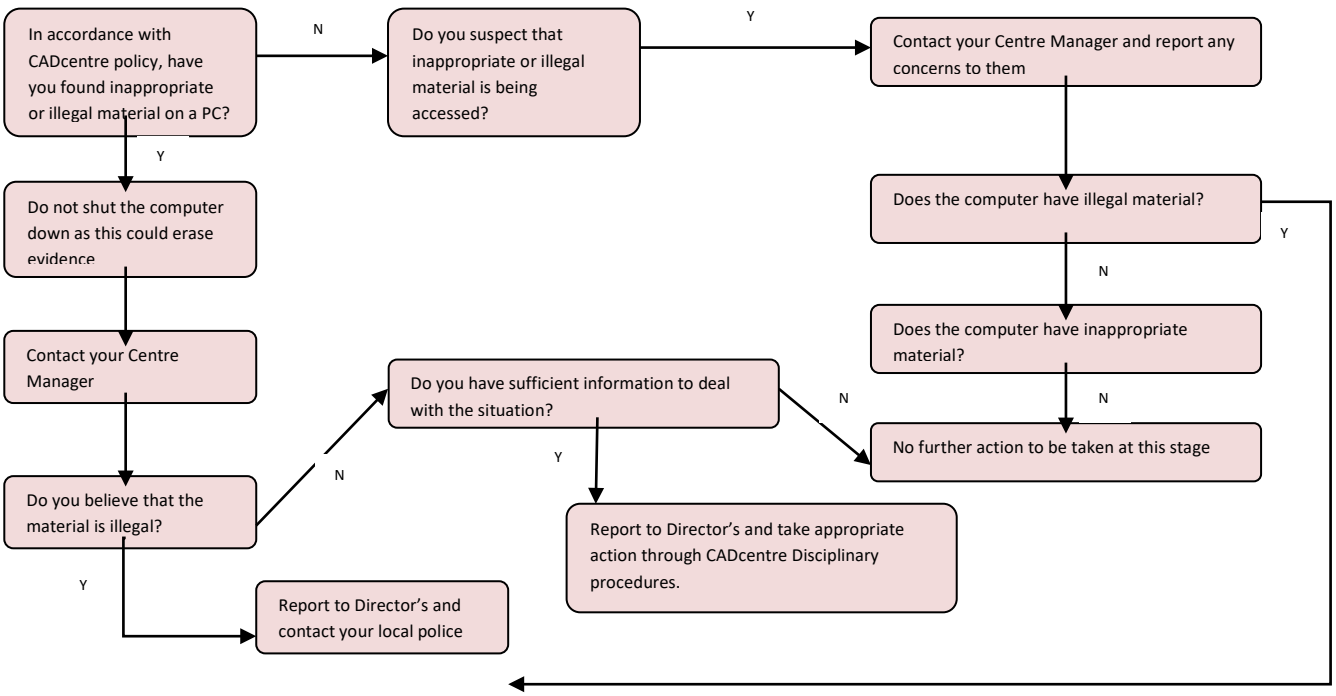
The CADcentre believes that the activities referred to in the following section would be inappropriate in a training context and that users, as defined below, should not engage in these activities when on CADcentre premises or

when using CADcentre equipment or systems. The CADcentre policy restricts certain internet usage as follows; Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images
- Promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse or fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK
- Criminally racist material
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred, extremism or acts of terrorism.
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the CADcentre or brings the CADcentre into disrepute
- Using CADcentre systems to run a private business
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential information e.g. financial/personal information, databases, computer passwords etc
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gaming, On-line gambling, On-line shopping
- File sharing
- Use of social networking sites or use of video broadcasting e.g. youtube

Responding to incidents of misuse

It is hoped that all learners, staff and visitors of the CADcentre will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse. If any apparent or actual misuse appears to involve illegal activity, the flow chart below should be consulted and actions followed in line with the flow chart, in particular the sections on reporting the incident to the police and the preservation of evidence.



If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the member of staff must contact the Centre Manager immediately and a full investigation will take place on a "clean" designated computer.

It is more likely that the CADcentre will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that staff/learners are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Legislation

Computer Misuse Act 1990
This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998
This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. See page 3 of this e-safety policy.

Communications Act 2003
Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988
It is an offence to send an indecent, offensive, or threatening letter, electronic communication to another person.

Regulation of Investigatory Powers Act 2000
It is an offence for any person to intentionally and without lawful authority, intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The CADcentre reserves the right to monitor its systems and communications in line with its rights under this act.

Copyright, Designs and Patents Act 1988
It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small

amounts for non-commercial research or private study. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984
It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994
This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006
This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

Protection of Children Act 1978
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003
The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust).

Public Order Act 1986
This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Obscene Publications Act 1959 and 1964
Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

The Counterterrorism and Security Act 2015.
This puts a statutory duty on public bodies and schools, FE colleges, and Work Based learning providers to have due regard to prevent people being drawn into radicalisation, extremism and terrorism.

Director’s Signature: