IC Training Centre

E_Safety Policy

INTRODUCTION

E-safety is defined as being safe from risks to personal safety and wellbeing when using all fixed and mobile devices that allow access to the internet, as well as those that are used to communicate electronically. This includes personal computers, laptops, mobile phones and gaming consoles such as Xbox, Playstation and Wii. Safeguarding against these risks is not just an ICT responsibility, it is everyone's responsibility and needs to be considered as part of overall arrangements in place that safeguard and promote the welfare of all individuals, particularly those that are vulnerable.

Our E-safety Policy builds on best practice and government guidance. It relates to the latest version of DfE statutory guidance: 'Keeping Learners Safe in Education 2021', Local Authority **Safeguarding Children Partnership (SCP)** and E-safety Guidance and Procedures.

Cyberbullying by learners will be treated as seriously as any other type of bullying and will be managed through our Anti-bullying Policy and Behaviour Policy.

UNDERSTANDING THE RISKS OF USING THE INTERNET AND ASSOCIATED DEVICES

The internet is an essential element in 21st century life and ICT knowledge, now seen as an important life-skill, is vital to access life-long learning and employment. It is also important to recognise that the internet provides many benefits, not just to learners, young people and vulnerable adults, but also to the professional work of staff.

E-safety covers the Internet, but it also covers mobile phones and other electronic communications technologies. We know that some adults and young people will use these technologies to harm learners or vulnerable adults. The harm might range from sending hurtful or abusive texts and emails, to enticing learners to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with learners and young people and educating all members of staff the on the risks and responsibilities of E-safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating ICT activity in IC Training Centre and provide a good understanding of appropriate ICT use that members of the IC Training Centre community can use as a reference for their conduct online outside of teaching hours. E-safety is a whole-IC Training Centre issue and responsibility.

While acknowledging the benefits, it is also important to recognise that risk to safety and well-being of users is ever- changing as technologies develop. These can be summarised as follows:

Content

- Commercial (adverts, spam, sponsorship, personal information)
- Aggressive (violent/hateful content)
- Sexual (pornographic or unwelcome sexual content)
- Values (bias, racism, misleading info or advice)

Contact

- Commercial (tracking, harvesting personal information)

- Aggressive (being bullied, harassed or stalked)
- Sexual (meeting strangers, being groomed)
- Values (self-harm, unwelcome persuasions)

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams, terrorism)
- Aggressive (bullying or harassing another)
- Sexual (creating and uploading inappropriate material, including sexting)
- Values (providing misleading info or advice)

Much of the material on the internet is published for an adult audience and some is unsuitable for younger or more vulnerable people. In addition, there is information on weapons, crime, racism and extremism that would be considered inappropriate and restricted elsewhere. It is also known that adults who wish to abuse others may pose as a child/young person/peer to engage with them and then attempt to meet up with them. This process is known as 'grooming' and may take place over a period of months using chat rooms, social networking sites, tablets and mobile phones.

CYBERBULLYING

Cyberbullying is bullying through the use of communication technology and can take many forms e.g., sending threatening or abusive text messages, e-mails or through messaging within social media websites. This bullying can be either personally or anonymously directed at individuals, making insulting comments about someone on a social networking site or blog or making/sharing derogatory or embarrassing videos of someone via mobile phone or e- mail.

SEXTING

This involves users sending sexually explicit texts in the form of images or video to other learners or adults. These images are often then distributed further without permission, which poses a significant safeguarding risk and places them at risk of further harm.

WHY INTERNET AND DIGITAL COMMUNICATIONS ARE IMPORTANT

Teaching and learning:

- The Internet is an essential element in 21st century life for education, business and social interaction. IC Training Centre has a duty to provide learners with quality Internet access as part of their learning experience.
- We believe that the use of Internet and is a necessary tool for staff and learners. The learners learn how to use the internet to find, search, exchange and share information.
- Learners will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- Learners will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Learners will be shown how to publish and present information appropriately to a wider

audience.

Learners will be taught how to evaluate Internet content

- IC Training Centre will seek to ensure that the use of Internet derived materials by staff and by learners complies with copyright law.
- Learners will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Learners will be informed of how to report unpleasant Internet content.

In addition to accessing the internet in organisation settings, learners, young people and vulnerable adults may access the internet and/or use other digital technologies in their own time at other locations. This is when they will be at greater risk if they have not been taught about how to use them safely and what the dangers are.

ROLES AND RESPONSIBILITIES

Managing Director Jayabalan Gukanesan

Responsible for the approval of the E-safety policy and for reviewing the effectiveness of the policy by reviewing E-safety incidents and monitoring reports.

- Ensure an E-safety policy is in place, reviewed every year (or earlier if required) and is available to all stakeholders
- Ensure that there is an E-safety coordinator who has been trained to a higher level of knowledge which is relevant to IC Training Centre, up to date and progressive
- Ensure that procedures for the safe use of ICT and the Internet are in place and adhered to
- Hold SMT and staff accountable for E-safety.

Centre Manager Rupal Mehta

The Centre Manager has a duty of care for ensuring the safety (including E-safety) of members of the IC Training Centre community, though the day-to-day responsibility for E-safety. Any complaint about staff misuse must be referred to the Managing Director.

- Ensure access to induction and training in E-safety practices for all users.
- Ensure appropriate action is taken in all cases of misuse.
- Ensure that Internet filtering methods are appropriate, effective and reasonable.
- Ensure that staff or external providers who operate monitoring procedures be supervised by a named member of SMT.
- Ensure that learner or staff personal data as recorded within IC Training Centre management system sent over the Internet is secured.
- Ensure the ICT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly.

- The Senior Management Team will receive monitoring reports from the IT Technician.

IT Support Saravanan Natarajan

IT Support is responsible for ensuring:

- That IC Training Centre technical infrastructure is secure and is not open to misuse or malicious attack.
- That IC Training Centre meets required E-safety technical requirements and any relevant body E-safety policy / guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- That they keep up to date with E-safety technical information in order to effectively carry out their E-safety role and to inform and update others as relevant.
- That the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in IC Training Centre policies.
- Updating of the relevant virus protection.
- Discussing security strategies with the Local Authority, Internet Service Provider and other agencies

E-mail

- Learners and staff may only use approved e-mail accounts which will be checked to ensure they offer added protection of information sharing.
- Learners must immediately tell a member of staff if they receive offensive e-mail.
- Learners must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone they meet online.
- Staff to learner email communication must only take place via a IC Training Centre email address and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- IC Training Centre will consider how e-mail from learners to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.
- Staff to staff e-mails concerning learners should use initials as identification, not names.

PUBLISHING LEARNER'S IMAGES AND WORK

Images or videos of learners are considered to be forms of personal information

Written permission will be obtained before photographs or videos of learners are used in IC Training Centre or published on the website. Where appropriate, permission will be obtained from parents or carers.

SD cards, memory sticks and CDs are a temporary means of storage for images. Once they have been used or uploaded to a secure location (e.g., the IC Training Centre network) they should be removed from the temporary storage device.

Images obtained via a third party are subject to copyright and either verbal or written permission should be obtained before they are used.

Reminders will be given that photographs and videos taken must be retained only for personal use and not posted online without express permission of the individual shown.

Social networking and personal details

- IC Training Centre will limit access to social networking sites and consider how to educate learners in their safe use e.g., use of passwords.
- Learners will be advised never to give out personal details of any kind which may identify them or their location.
- Learners will be advised to use nicknames or avatars when using social networking sites.

Managing filtering and access to inappropriate content

- IC Training Centre will work in partnership to ensure systems to protect learners are reviewed and improved in line with the most recent guidance.
- If staff or learners come across unsuitable on-line materials, the site must be reported to a member of the Senior Management Team.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- Class Member of staffs and Trainers will be responsible for overseeing the content that learner's access, particularly in places outside of the classroom (corridor computers or use of portable technologies) or at times outside of lessons

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and the potential risks assessed before use in IC Training Centre is allowed.
- Learners will not use personal mobile phones and associated cameras during lessons or formal IC Training Centre time. The sending of abusive or inappropriate text messages is forbidden.
- Games machines which have Internet access which may not include filtering will be strictly monitored. Care will be taken with their use within the IC Training Centre.

- Staff will use a IC Training Centre phone where contact with learners is required.

PROTECTING PERSONAL DATA

IC Training Centre is responsible for reviewing and managing the security of the computers and Internet networks and we have rigorous policies and procedures in place, as well as having achieved Cyber Essentials accreditation. We take the protection of data and personal protection very seriously, which means protecting the IC Training Centre network, as far as is practicably possible, against viruses, hackers and other external security threats. Together with our external specialists, the IT Manager will review the security of the information systems and users regularly and virus protection software will be updated regularly.

Some safeguards that IC Training Centre takes to secure our computer systems are:

- Ensuring that all personal data sent over the Internet or taken off site is encrypted
- Making sure that unapproved software is not downloaded to any IC Training Centre computers. Alerts will be set up to warn users of this
- Files held on the IC Training Centre network will be regularly checked for viruses
- The use of user logins and passwords to access the IC Training Centre network will be enforced
- Portable media containing IC Training Centre data or programmes will not be taken off-site without specific permission from the Managing Director

For more information on data protection in IC Training Centre please refer to our **Data Protection / GDPR policy**.

DATA STORAGE AND TRANSPORT

All personal information must be kept secure. IC Training Centre employ a combination of technical and procedural solutions to maximise the security of personal data (including photographs) of learners or adults:

- All staff laptops will be password protected and staff will be encouraged to change these regularly.
- Transporting personal information off site should be avoided unless necessary.
- If personal data is required to be taken off site, it should either be stored on a password protected laptop or an encrypted memory stick and be deleted when no longer needed.

POLICY DECISIONS AUTHORISING INTERNET ACCESS

- All staff must read and sign the **'Staff Acceptable Use Agreement'** before using any IC Training Centre ICT resource or personal device in IC Training Centre.
- IC Training Centre will maintain a current record of all staff and learners who are granted access to IC Training Centre ICT systems.
- Any learner who is deemed a high risk when using the Internet or any ICT equipment / resource will have restricted access in IC Training Centre

- Any person not directly employed by IC Training Centre will be reminded of the 'acceptable use of IC Training Centre ICT resources' before being allowed to access the Internet. Use of ICT resources will be monitored closely.

ASSESSING RISKS

- IC Training Centre will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a IC Training Centre computer. IC Training Centre cannot accept liability for the material accessed, or any consequences of Internet access.
- IC Training Centre will audit ICT use to establish if the E-safety policy is adequate and that the implementation of the E-safety policy is appropriate and effective.

HANDLING E-SAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Director of Corporate Training
- Complaints of a child protection nature must be dealt with in accordance with IC Training Centre's Safeguarding procedures.
- Where appropriate, learners and parents will be informed of the complaint's procedure.
- Where appropriate, learners and parents will be informed of consequences for learners misusing the Internet.

COMMUNICATIONS POLICY

Introducing the E-safety policy to learners

- Appropriate elements of the E-safety policy will be shared with learners.
- E-safety posters will be posted nearby to where computers or mobile devices may be used.
- Learners will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of E-safety issues and how best to deal with them will be provided for learners.

STAFF AND THE E-SAFETY POLICY

- All staff will be directed to read IC Training Centre's E-safety Policy and its importance explained.
- All members of staff will be asked to sign the **Acceptable Use Agreement**.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

REVIEW

This policy will be reviewed on an annual basis or following changes to Government updates and statutory guidance in relation to Covid-19 and company risk assessment policies and processes.

ACCEPTABLE USE AGREEMENT

This Policy has been written by the IC Training Centre, involving all stakeholders and builds on best practice and government guidance. Our Acceptable Use Agreement builds on best practice and government guidance. It relates to the latest version of DfE statutory guidance: 'Keeping Learners Safe in Education 2021', and **Local Safeguarding Children Partnership (BSCP)** and E-safety Guidance and Procedures.

This agreement should also be read in conjunction with the most recent version of **IC Training Centre's Staff Handbook,** which sets out the **Staff Code of Conduct**, use of electronic devices and social networking sites, safeguarding learners and our expectations for upholding the highest standards of professional conduct both in and outside of the IC Training Centre workplace.

The aims of this policy are:

- To encourage safe use of the Internet by both young people and adults working within our IC Training Centre.
- To encourage the development of skills to access, analyse and evaluate resources from the Internet.
- To use these resources to support teaching and learning across the curriculum.
- To ensure their supervised and appropriate use.

GUIDELINES

As access can lead to any publicly available resources on the Internet, a filtered/screened service may be used in IC Training Centre to block access to the majority of unsuitable sites. This will ensure access to unsuitable material is minimised.

Learners will be shown how to find and access information on suitable web search engines, such as 'Google'.

All staff members will be aware of their responsibilities towards learners, checking sites they recommend are suitable, ensuring that access is supervised and that appropriate rules are being followed.

In so far as possible, screens should always be facing the member of staff. Where this is not the case the member of staff must walk regularly around the group to supervise sites being accessed. Learners should be aware of the problems associated with Internet access and should be encouraged as a class to develop their own Internet rules before the class uses the Internet. They should know that by using 'history' and 'cookies', the member of staff can review what has been accessed.

If possible, a written record is to be kept of any undesirable material that is accessed inadvertently. Contact with the ISP will be made if necessary, to adjust filtering settings.

E-MAILS

No e-mail should be sent from the IC Training Centre without a member of staff approving it. Learners should be identified by the name in the subject area of the e-mail, not in the address. Assessor's / Trainers / Member of staffs are responsible for the e-mail that is received by their class.

The use of Chat rooms to support teaching and learning will be closely monitored to protect against incidents of cyberbullying. Learners will be taught, as stated in the E-safety Policy, about keeping themselves safe when using the Internet.

VIRUS PROTECTION

Virus protection is installed and kept up to date in IC Training Centre (Sophos Anti-Virus). Computer users, especially Internet users, should be aware of the dangers of virus corruption from Internet downloads or attachments to e-mails. Daily virus updates to the IC Training Centre network will be used to help prevent damage to files and systems.

INTERNET AND SYSTEM MONITORING

All Internet activity is monitored by IC Training Centre system and checked by IC Training Centre's ICT technician. It is their responsibility to review this activity periodically and report any transgressions of IC Training Centre's Internet policy and/or use of obscene, racist or threatening language detected by the system to the Managing Director. Occasionally, it may be necessary for the ICT technician to investigate attempted access to blocked sites, and in order to do this, they will need to set his/her Internet access rights to "Unrestricted". Whenever this happens, this should be recorded in the ICT violations register, and the Managing Director notified.

Any serious transgressions of IC Training Centre's E-safety Policy will be recorded and dealt in accordance with the IC Training Centre's Behaviour Policy or for adults, the relevant Safeguarding Policy, or Staff Code of Conduct.

INTERNET PUBLISHING STATEMENT

IC Training Centre wishes our website to reflect the range of activities and educational opportunities on offer, however, we recognise the potential for abuse that material published on the Internet may attract, no matter how small this risk may be. Therefore, when considering material for publication, the following conditions should be adhered to:

- No photograph or video recording may be published without the written consent of the parents/legal guardian of the child concerned, and the child's own verbal consent.
- Surnames of learners should not be published, especially in conjunction with photographic or video material
- No link should be made between an individual and any home address (including simply street names)
- Where the person publishing material suspects that there may be child protection issues at stake then serious consideration must be taken as to whether that material may be published or not. In the case of a simple piece of artwork or writing, this may well be fine, but images of that person should not be published. If in any doubt at all, refer to the Designated Safeguarding Lead.

STAFF AND VOLUNTEERS MUST ABIDE BY THE FOLLOWING CODE OF CONDUCT

- This covers use of digital technologies in the organisation i.e., e-mail, internet, intranet and network resources, learning platforms, software, mobile technologies, equipment and systems.

- I will only use the organisation's digital technology resources and systems for professional purposes or for uses deemed reasonable by the manager.
- I will only use secure e-mail system(s) for any organisation's business (web mail accounts are not secure e- mail system(s)).
- I will not browse, download or send material that could be considered offensive to colleagues and any other individuals.
- I will report any accidental access, receipt of inappropriate materials or filtering breaches to the manager.
- I will not allow unauthorised individuals to access e-mail / internet / intranet /networks or systems.
- I will ensure that all my login credentials (including passwords) are not shared with any other individuals, displayed or used by any individual than myself.
- I will not download any software or resources from the internet that can compromise the network or are not adequately licensed.
- I will ensure that my personal e-mail accounts, mobile/home telephone numbers are not shared with learners, young people or families.
- I will not allow learners and young people to add me as a friend to their social networking site nor will I add them as friends to my social networking site.
- I will ensure that any private social networking sites / blogs etc. that I create or actively contribute to are not confused with my professional role.
- I will ensure that the reputation of the IC Training Centre is not brought into question, following any messages, blogs or posts I may make online.
- I understand that all internet and network usage can be logged, and this information could be made available to my manager on request.
- I will not connect a computer, laptop or other device to the network/internet that has not been approved by the organisation and meets its minimum-security specification.
- I will not use personal digital cameras or camera phones for transferring images of learners and young people or staff without permission.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that the Data Protection Act requires that any information seen by me with regard to staff or learners and young people, held within any organisation system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will at all times behave responsibly and professionally in the digital world and will not publish any work- related content on the internet without permission from the Head of

department.

- I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice.
- I understand that failure to comply with this Acceptable Use Agreement (AUA) could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the organisation's most recent Acceptable Use Agreement.

I agree to abide by the organisation's most recent Acceptable Use Agreement.

Signature ………………………………………………… Date ……………………

Full Name……………………………………………………………………(print)

Job title ……………………………………………………………………………………

6/1/23.