1. CONTENT

1.1 E-safety Strategy for Hull – The City perspective

The digital world our children and learners live in is a rapidly changing place. New technologies are creating fantastic, exciting opportunities in communication, in learning and in many aspects of daily life. For many adults these developments seem quite different from what we have seen before. This makes us naturally cautious about them. However, for learners they are a regular and familiar part of everyday life that is being enthusiastically embraced. This gives those of us whose role it is to safeguard our children and learners new considerations, challenges and new responsibilities. We want them to flourish through the many benefits that the digital world can offer. Yet at the same time we must help them understand and make informed decisions about what information they seek and share, the way that they do this and who they do it with.

We are clear about this responsibility and under the guidance of the Hull Safeguarding Children's Partnership E-safety work stream we have developed the E-safety Strategy to give coherence and focus to our work, providing a safe, city-wide framework. The E-safety Strategy recognises the role developments in digital technology play in shaping the way learners access ICT, highlighting the importance of helping learners understand what constitutes acceptable use. Crucially, it focuses on building the resilience of learners in using digital technology, so they are equipped to enjoy the benefits and avoid the pitfalls and dangers.

When working in a field as complex and fast changing as e-safety, we must personalise the support we provide so that each individual child or young person has the skills and understanding to use digital technology safely. We must seek the participation of children, learners and families so we can appreciate the changing nature of their usage and respond accordingly. We must work in partnership, to deliver a coherent approach with a particular focus on bringing everyone together around this common agenda. Finally, we must come back to our responsibility – prevention - helping learners to ensure that they are able to identify, avoid and report dangers before they escalate. This is not always easy, the pace of change means that as adults we can be in danger of feeling out-of-touch with and confused by technologies that learners are using. However, the onus is on us to overcome these potential barriers and take a balanced, responsible view.

Funded by
Education & Skills Funding Agency
European Union
European Social Fund

Under the Children Act 2004 Section 11 and the Education Act 2011 all professionals have a duty to safeguard and promote the well being of all children. This duty of care to safeguard and promote the welfare of children and learners cannot be confined to a single environment. E-safeguarding must extend to all environments in which children and learners actively engage with the digital world, in college or training, at home or through personal use within the wider community. This requires an integrated approach across learning establishments and other establishments in Hull (herein after described as "organisations") that regularly come into contact with learners. Our strategy is to develop safety and responsibility in the digital world, and to educate and empower children and learners to identify and mitigate risk. The strategy requires colleges and other learning establishments, parents, carers, pupils and other professional organisations coming into contact with children, to sign-up to the principles contained within this document, the policies underpinning it and to respond effectively to any incidents arising.

1.2 National Context

The Byron Review *Safer Children in a Digital World: The Report of the Byron Review* 2008, investigated the issues and opportunities for keeping children and learners safe in their use of digital technologies. The report highlighted the benefits the digital world provides but also the risks surrounding potentially inappropriate material. Such online risks can be classified in terms of **content**, **contact** with others and **conduct** of children in the digital world, illustrating that e-safety risks are posed more by behaviours and values online than the technology itself. As such, a child may be a recipient, participant or actor in online activities posing risk.

The Byron report concluded that our approach to children and learners' use of technology must shift: rather than restricting access to technology, we need to not only 'reduce the availability of potentially harmful material' but also, 'restrict access to it by children' and 'increase children's resilience' and in doing so empower learners to develop safe and responsible on line behaviours to protect themselves whenever and wherever they go online.

Keeping Children Safe in Education, provided further guidance to schools and colleges. There is an additional need to ensure children and young people are protected from radicalisation and duties under PREVENT are met (see safeguarding policies).

1.3 What do we mean by e-safeguarding?

E-safeguarding procedures address all safeguarding issues which relate to the use of digital technology. There are two main elements to these issues:

E-safety
E-safety stands for electronic safety, it is not just about keeping safe on the internet but also keeping safe on all electronic devices such as mobile phones, tablets, television *etc*. All organisations require procedures to understand rights and responsibilities in using digital technology safely. These procedures are expressed in our organisation's Acceptable Use Policy (AUP). The AUP policy is referred to as the 'Guidance on the use of IT Policy' within the City Council.

E-security
E-security refers to the protection of data against the deliberate or accidental access by unauthorised persons, and also includes protection against accidental damage or loss. All organisations require procedures to protect the physical network infrastructure to ensure all information and electronic data is securely maintained and is categorised as Public, Restricted or Protected.

1.4 The place of Acceptable Use Policies

Effective Acceptable Use Policies (AUPs) are an essential tool to promote safe and responsible behaviours online in organisational settings, the home and for those who provide services to children and learners. AUPs state the way in which new and emerging technologies may and may not be used and the sanctions for misuse. It is important that AUPs are developed within a framework of wider e-safety measures and within their local context. These measures involve the combined approach of effective policies and practice, a robust and secure technology infrastructure, and education and training for both children and adults alike, all underpinned by standards and inspection.

1.5 The Hull E-safety Toolkit

There are many aspects to keeping safe online. All agencies and organisations working with children and learners will be dealing with the policies, infrastructure, and education they need to put in place to ensure e-safety at a personal, organisational, network and data security level. Parents/carers will need to understand the risks learners may be exposed to, and how they can supervise and support their children effectively. Learners themselves will need to develop the skills to evaluate the way they use technology at home and at college, identify those risks and develop ways to balance the risks with the benefits.

2.0 Guidance

Our E-safety Guidance and Acceptable Use Policies build upon the Hull City Council's (HCC) Policy on the use of Information Technology and government guidance and are in accordance with Hull Safeguarding Children's Partnership's Guidelines and Procedures.

2.1 Empowering Learners in the Digital World

2.1.1 Why is Internet use important?
Learners will experiment online, to enable them to take advantage of the many educational and social benefits of new technologies. Learners need opportunities to create, collaborate and explore in the digital world, using multiple devices from multiple locations. However, all users need to be aware of the range of risks associated with the use of these internet technologies alongside the development of safe and responsible online behaviours.

The rapid developments in electronic communications are having many effects on society. It is important to state what we are trying to achieve in the Service through digital technology.

- The Internet is a part of everyday life for education, business and social interaction. The Service has a duty to provide learners with Internet access.
- Learners use the Internet widely outside the training and education venues and need to learn how to evaluate Internet information and to take care of their own safety and security.
- The purpose of Internet use across the Service is to raise educational standards, to promote learners' achievement, to support the professional work of staff and to enhance the Service management functions.

2.1.2 How can we ensure Internet use enhances learning and life experiences?

Increased computer numbers and improved Internet access may be provided but its impact on learning outcomes should also be considered. Developing effective practice in using the Internet for teaching and learning is essential. Learners need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet. Respect for copyright and intellectual property rights, and the correct use of published material should be taught. Methods to detect plagiarism will be used as part of assessment review. .

- The Service Internet access will be designed to enhance and extend education.
- Learners will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- The Service will ensure that the copying and subsequent use of Internet derived materials by staff and learners complies with copyright law.
- Access levels will be reviewed to reflect the curriculum requirements and age of the learners.
- 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 taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- Learners will have individual accounts created (with the exception of those on short courses of 10 weeks or less) to enable any misuse on the internet to be readily identified and dealt with.

2.1.3 How will learners learn how to evaluate content?

The quality of information received via radio, newspaper and telephone is variable and everyone needs to develop critical skills in selection and evaluation. Information received via the Internet, email or text message requires even better information handling and digital literacy skills. It may be difficult to determine origin, intent, and accuracy, as the contextual clues may be missing or difficult to read. In training providers, a whole curriculum approach may be required.

The extent to which the internet is used by extremists as a tool for radicalisation is not fully known, but it is clear that persons responsible for recent attacks have accessed and been influenced by the internet to varying degrees.

The internet and social networking sites may provide a virtual online community to which a learner may wish to belong and then may in turn become increasingly exposed to extremism. Extremist websites may be used to disseminate propaganda, spread news and updates on extremist issues, add radical interpretation to theological tracts and provision of discussion forums for likeminded individuals. The internet also offers easily accessible downloadable extremist material including advice and guidance on bomb making are often filtered out of public systems, but usually not at home – policies need to empower learners to evaluate content critically.

- Learners should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of teaching/learning in every subject.

2.2 Managing Information Services

2.2.1 How will information systems security be maintained?

Each authorised user of the Council's information technology facilities is responsible for ensuring that security is maintained by ensuring that equipment is not left logged-on at the end of the day and that rules relating to password security are strictly adhered to.

It is the duty of all users to immediately report suspicious activities and actual or suspected breaches of information security as described in the Council's Information Security Policy. Employees must immediately report any misuse or irresponsible actions that affect the security of work data or information to their line manager.

All staff with access to personal data are liable in law to protect that data. Information is used throughout the Service and is sometimes shared with external organisations and applicants. The use of removable media may result in being unable to access information, or interference with the integrity of information, which could have a significant effect on the efficient operation of the Service and may result in financial loss and an inability to provide services.

Use of removable media for data transfer should not be used unless it is an encrypted device. Removable media devices include, but are not restricted to the following;

- CDs, DVDs, floppy and optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives).
- Media Card Readers
- Embedded Microchips and storage cards (including those on mobile phones and PDAs – also known as memory cards)
- MP3 and other music/media players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)

and any other device that transfers data between systems, or stores electronic data separately from email or other applications.

Use and Security of ICT systems

Access to all ICT systems shall be via unique login and password.
All requests for access beyond that normally allocated:

- All staff have access to learners' personal storage
- Staff needing to access another member of staff's personal storage due to e.g. sickness, shall be authorised by their line manager.

This shall include the authorisation of access required by the ICT Support Team during investigations.

≈ All access controls should be reviewed each term, to ensure that any users that leave have their access removed. Information Technology use is monitored and where suspected misuse occurs, detailed investigations will be undertaken.

≈ Please note that failure to comply with the Council's Policy, Procedure and Guidance on the use of Information Technology may constitute gross misconduct and could lead to dismissal.

≈ In the interests of security employees must make secure their personal computer (PC) if leaving the PC unattended. There are 2 main ways of securing a PC during the day:-

- Logging Out - suitable for substantial absences from the workplace. This is done by pressing CTRL-ALT-DELETE and selecting 'Lock Computer' or Log Off, or by pressing the Windows key together with the L key.
- Lock Computer - available on Windows XP and above. Suitable for lunch-breaks, meetings, etc. This utility can be invoked at any time on the PC and leaves all open or running activities on the PC uninterrupted. It can only be circumvented by an authorised high-level user or by re-starting the PC (but this would simply bring the PC to its normal login state).

This would ensure that in the event of an unplanned absence from the PC it would automatically protect itself. On Windows XP and above it is deactivated by the usual login password.

≈ Servers are located securely and physical access restricted.

≈ Virus protection for the whole network is installed and current.

≈ Access by wireless devices must be pro-actively managed and must be password protected

≈ Portable media on the Hull Training network may not be used without specific permission followed by a virus check.

≈ Unapproved software and unlicensed software is not allowed in any work areas or attached to email.

≈ Files held on the organisation's network are regularly checked.

≈ The ICT Support team will review system capacity and report to the Senior Management team.

Space on servers is at a premium and is costly to administer and backup, therefore, the Service information technology facilities must not be used to store any non-work related information i.e. personal data, photographs, downloads or files.

When employees leave the Service, their user accounts will automatically be closed immediately. Any information that employees have saved in any form on PCs, network servers, or in Outlook will still be available for managers to request for up to 90 days through a service desk request. After this time any remaining data will be permanently deleted.

Information stored on the c: drive on PCs or laptops is not normally backed up and may be lost at any time and is, therefore, not as secure as that stored on the network. Information that is important or confidential or is sensitive personal information should not, therefore, be stored on this area of the system.

≈ Where any external network traffic is allowed from the Internet to the organisation, a local firewall is deployed to restrict traffic to only necessary ports and IP addresses.
≈ All wireless implementations shall be a minimum of WPA 2 encryption, and shall require authentication prior to connection.
≈ The security of the Service information systems and users will be reviewed regularly, at least annually.

2.2.2 How will filtering be managed?

In order to protect the Service from possible litigation and also the risk of overloading the servers have software which allows it to filter and block certain Internet sites so that staff and learners are unable to access them. Categories of sites include:

- Adult/Mature content
- Chat/Instant Messaging
- Gambling, Hacking
- Illegal Drugs
- Nudity
- Extremism/radicalisation

Several other categories of sites of a similar nature will also be blocked.

≈ Blocking strategies prevent access to a list of unsuitable sites. Maintenance of the blocking is done automatically by the filtering software installed on the server.
≈ Access monitoring records the Internet sites visited by individual users.
≈ The Service will work with HCC or the ICT support team to ensure that systems to protect learners are reviewed and improved.
≈ A senior member of staff in the organisation will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.

Where applicable, loaned equipment such as Chromebooks and laptops will be monitored by HTAE when used onsite and off. Web activity will be monitored, filtered and in some cases, blocked using the same categories outlined above.

Any inappropriate searches/content in relation to the Prevent Agenda (including extremism/radicalisation) will be reported to Channel by the Safeguarding and Learner Support Manager/Designated Safeguarding Lead in line with the HTAE Adult and Child Safeguarding Policies.

2.2.3 How will emerging technologies be managed?

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, collaboration, and multimedia tools. This can offer immense opportunities for learning as well as dangers, such as learners using a phone to video others. A risk assessment will be undertaken on each new technology for effective and safe practice in classroom and/or Service use.

Virtual online classrooms and communities widen the geographical boundaries of learning. Approaches such as mentoring, online learning and parental access are becoming embedded within provider's systems. Online communities can also be one way of encouraging a disaffected pupil to keep in touch.

The safety and effectiveness of virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the provider may be difficult as demonstrated by social networking sites such as Bebo, MySpace and Facebook. The registering of individuals to establish and maintain validated electronic identities is essential for safe communication but is often not possible.

The Service will keep up to date with new technologies, including those relating to mobile phones and hand-held devices, but develop appropriate strategies. For instance, text messaging via mobile phones is a frequent activity for many learners and families; this could be used to communicate a learner's absence or to send reminders. There are dangers for employees/volunteers however if personal phones are used to contact learners and therefore an organisationally owned phone should be issued.

The inclusion of inappropriate language or images is difficult for adults to detect. Learners may need reminding that such use is inappropriate and conflicts with the organisational policy. Abusive messages should be dealt with under the organisation's behaviour and/or anti-bullying policies.

2.3 Privacy and Protection

2.3.1 How should personal data be protected?

The Data Protection Act 2018 ("the Act"), updated by General Data Protection Regulations (GDPR) gives individuals the right to know what information is held about them, who it is shared with and provides a framework to ensure that personal information is handled/retained properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information

(personal data) must notify the Information Commissioner's Office, unless they are exempt. Please also see the Privacy Statement on the Hull Training & Adult Education website. https://www.hcctraining.ac.uk/privacy/

The Data Protection Act 2018 applies to anyone who handles or has access to information concerning individuals. Everyone in the workplace has a legal duty to protect the privacy of information relating to individuals.

The Act sets standards (eight data protection principles), which must be satisfied when processing personal data (information that will identify a living individual).

The Act also gives rights to the people the information is about *i.e.,* subject access rights let individuals find out what information is held about them. The eight principles are that personal data must be:

- Processed fairly and lawfully;
- Processed for specified purposes;
- Adequate, relevant and not excessive;
- Accurate and up-to-date;
- Held no longer than is necessary;
- Processed in line with individual's rights;
- Kept secure; and
- Transferred only to other countries with suitable security measures.

All data from which people can be identified must be protected. Hull City Council Data Protection information may be seen at www.hullcc.gov.uk.

2.3.2 Password security

All members of staff/volunteers with access to ICT systems shall be responsible for taking the appropriate steps to select and secure their passwords.

These steps are described in Hull City Council's Policy and Guidance on the Use of information technology. Staff/volunteers must:

- Keep their password secure from others.
- Follow the password style of HCC
- Changing passwords as requested by HCC
- In addition, when leaving a computer for any length of time, all staff members/ volunteers shall log off or lock the computer, using CTRL+ATL+DELETE or other system command.

2.3.3 How will email be managed?

The implications of email use for the Service by learners need to be managed and appropriate safety measures put in place. Un-regulated email can provide routes to learners that bypass the traditional Service boundaries.

Restriction of incoming and outgoing email to approved addresses and filtering for unsuitable content is undertaken.

In the organisational context, email should not be considered private and most organisations reserve the right to monitor email. Refer to paragraph on page 8 – 'Security on IT systems'

Emails will be created for Microsoft 365 to show learner first initial and surname eg jsmith@hulltraining.ac.uk. Email accounts should not be provided which can be used to identify learners e.g., full name and their organisation. E Safety briefings to learners must include information on keeping secure and the appropriate use of emails.

- Learners may only use approved email accounts.
- Learners must immediately tell their tutor if they receive offensive email.
- Access in college/organisation to external personal email accounts may be blocked.
- Excessive social email use can interfere with learning and is locked.
- Email sent to external organisations should be written carefully and, if it contains potentially contentious information, authorisation should be sought before sending, in the same way as a letter written on Service headed paper.
- The forwarding of chain messages is not permitted.
- The Service will have a dedicated email for reporting well being and pastoral issues and this inbox must be approved and monitored by members of Senior Leadership Team/Senior Manager.

2.3.4 How will published content be managed?

Excellent websites can inspire learners to publish work of a high standard. Websites can celebrate learners' work, promote the Service and publish resources for projects.

Publication of information should be considered from a personal and the Service security viewpoint. Material such as employee/volunteer lists, or a plan, may be better published in a handbook or on a secure part of the website which requires authentication.

- Learners' personal information must not be published.
- Email addresses should be published carefully, to avoid being harvested for spam (e.g. consider replacing '@' with 'AT').
- The appointed senior leader will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The website should comply with the Service guidelines for publications, including respect for intellectual property rights and copyright.

2.3.5 `Can learner images and work be published?

Still and moving images and sounds add liveliness and interest to a publication, particularly when learners can be included. Nevertheless, the security of employee/volunteers and learners is paramount.

Images of learners should not be published without the appropriate written permission and adult learners must sign a release form before images can be used. Learners also need to be taught the reasons for caution in publishing personal information and images online.

- Learners' full names should not be used anywhere on the website, particularly in association with photographs.
- Signed release forms from parents or carers of minors will be obtained before images of learners are electronically published.
- Images of adult learners will not be used until they have signed a release form.

2.3.6 How will social networking and personal publishing be managed?

For responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Learners should be encouraged to think about the ease of uploading personal information, the associated dangers, and the difficulty of removing an inappropriate image or information once published.

All learners should be made aware of the potential risks of using social networking sites or personal publishing either professionally with learners or personally. They should be made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Examples include blogs, wikis, social networking, forums, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

- The Service will control access to social media and social networking sites.
- Learners will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, college attended, IM and email addresses, full names of friends/family, specific interests, and clubs etc.
- Learners should be advised on security and encouraged to set passwords, deny access to unknown individuals, and instructed how to block unwanted communications. Learners should be encouraged to invite known friends only and deny access to others by making profiles private.
- Learners are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

2.4 Risks and Responses

2.4.1 How will Internet access be authorised?

The Service will allocate Internet access for staff members/volunteers and learners on the basis of educational need.

- The organisation will maintain a current record of all staff/volunteers and learners who are granted access to the organisation's electronic communications.
- All staff/volunteers must read and sign the Hull City Council's policies regarding information security and the use of information technology before using the organisation's ICT resource.
- Learners must agree to comply with the Policy on the use of Information Technology.

2.4.2 How will risks be assessed?

E-security and e-safety is based upon the assessment of risk, and the implementation of controls to manage these risks; no use of digital technology is completely risk free. Information security is critical, in both protecting the information held concerning staff/volunteers and learners, and in ensuring the reliability of ICT systems to support teaching and learning.

A risk assessment shall be updated and reviewed annually by the Senior Leadership Team/Senior Manager of the organisation.

It is not possible to guard against every undesirable situation. The Service recognises that it is not possible to completely remove the risk that learners might access unsuitable materials via the system, however:

- The Service will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a computer.
- Neither the Service nor HCC can accept liability for the material accessed, or any consequences resulting from Internet use.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

2.4.3 How will complaints be handled?

Parents, staff and learners should know how to use the organisation's complaints procedure. The facts of the case will need to be established, for instance whether the Internet use was within or outside the organisation.

- Potential child protection and illegal issues will be referred to the Safeguarding and Learner Support Manager and the Designated Safeguarding Lead. Discussions shall be held with/between the Service, Children's Social Care, Police and Hull Safeguarding Children's Partnership to establish procedures for handling potentially illegal issues.
- Complaints of Internet misuse will be dealt with under HCC Complaints Procedure.
- Any complaint about staff misuse must be referred to the Head of Service.
- All e–safety complaints and incidents will be recorded by the Service — including any actions taken.
- Any issues (including sanctions) will be dealt with according to HCC disciplinary and child protection procedures.

2.4.4 How should the Internet be used across the community?

Staff will exchange views and compare policies with others in the community where learners are on placement with employers or volunteering.

- The Service will liaise with partner organisations to establish a common approach to e–safety.
- The Service will be sensitive to Internet related issues experienced by learners out of Service venues, e.g. social networking sites, and offer appropriate advice.

2.4.5 How will Cyber bullying be managed?

Cyber bullying can be defined as “The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone” Unfortunately, technologies can be used negatively. When learners are the target of bullying via mobiles phones, gaming, or the internet, they can often feel very alone, particularly if the adults around them do not understand cyber bullying and its effects.

Learners, adult learners, organisations, and parents/carers should be given information so that they understand how cyber bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

- Cyber bullying (along with all forms of bullying) will not be tolerated in the Service. Full details are set out in the Service policy on anti-bullying.
- All incidents of cyber bullying reported to the Service will be recorded.
- The Service will take steps to identify the bully, where appropriate, such as examining system logs, identifying, and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Sanctions for those involved in cyber bullying may include:
  - The bully will be asked to remove any material deemed to be inappropriate or offensive.
  - A service provider may be contacted to remove content.
  - Internet access may be suspended for the user for a period of time.
  - Parents/carers may be informed.
  - The Police will be contacted if a criminal offence is suspected.

2.4.6 How will Learning Platforms and VLEs be managed?

An effective learning platform (LP) or virtual learning environment can offer the Service a wide range of benefits to staff/volunteers, learners, parents/carers as well as support management and administration. It can enable learners and staff to collaborate in and across the organisation, can share resources and tools for a range of topics, create and manage digital content and develop online and secure e-portfolios.

- Senior Management Team/ Managers and staff/volunteers will monitor the usage of the LP by learners.
- Only members of the current learner, parent/carers and staff community will have access to the LP.
- All users will be mindful of copyright issues and will only upload appropriate content onto the LP.
- When staff, children and learners etc leave the Service their account or rights to specific areas will be disabled or transferred to their new establishment.
- A report button is available to report any concerns around safety and bullying/harassment

2.4.7 Response to an Incident of Concern

An important element of e-safeguarding is the ability to identify and deal with incidents of concern and related to the confidentiality of information. All staff/volunteers and learners have a responsibility to report e-safety or e-security

incidents so that they may be dealt with effectively and in a timely manner in order to minimise any impact. The Service has established an incident reporting procedure and records reported incidents in an Incident Log. This log is detailed 2.4.8

The Incident Log will be formally reviewed, and any outstanding actions delegated, by the Senior Management Team/Senior Manager responsible within the organisation at a minimum frequency of once per term. Through this review process, where deemed appropriate, management shall update the risk assessment in light of new incidents.

A list of common incidents include:

- Circumventing the network security system
- Accessing inappropriate material
- Installing unapproved software
- Using other people's accounts, email addresses or passwords
- Breaching copyright
- Uploading material onto a social network or chat room

Learners need to know how to block someone online and report them if they feel uncomfortable. It is important to realise that there are people other than the staff in your organisation who can help. Online child abuse can be reported directly, as well as requests to seek out more advice and support. Reports can be made directly to CEOP through their Click CEOP reporting button, which is present on an increasing number of websites and social networks.

2.4.8 E-incident Log Sheet

Member of staff identifying incident				
Date of incident:	Time of incident			
Duration of incident:	Do you know if repeat victim?	yes	no	unsure
Description of the e-safety incident: (please give as much information as you are able)				
Description of information recorded or secured				
Have files, audio/text/images been recorded and secured? Has any computer or other technology including phones been secured?		Yes	No	
If yes, how and where, who by and when?				
What actions were taken, and by whom? Give details of agencies informed and contact person within those agencies.				
Name of person completing this form:				
Organisation:				
Date:	Signature:			
For child protection issues send this form immediately to Designated Safeguarding Lead or, in their absence, to Learner services manager.				

01/09/2022

Head of Service ……... Date……

Sharon Gamble