|  |
| --- |
| W39657-Skills-For-Work-Banner-Oct2019SKILLS FOR WORK: e-SAFETY POLICY Aims   * Identify the roles and responsibilities relating to e-Safety at Skills for Work * Safeguard and promote the welfare of learners and staff * Help learners and staff take responsibility for their own e-Safety * Ensure staff and learners use technology safely and securely * Educate staff and learners about potential threats and harms arising from internet use   Skills for Work is committed to creating and maintaining a safe learning and working environment that promotes well-being and security for all its learners and staff within all locations by protecting their physical and psychological well-being and ensuring safeguarding from all forms of abuse. e-Safety is the process of limiting risks to young people and adults when using Information and Communications Technology (ICT). e-Safety is primarily a safeguarding issue not a technological issue, which relates to the use of all ICT- fixed or mobile; current, emerging and future ICT.  ICT is used daily as a tool to improve teaching, learning, communication and working practices. The use of ICT is of significant benefit to Skills for Work staff and customers, in personal, social, professional and educational contexts. How-ever alongside these benefits are potential risks that we have a duty of care to manage, to ensure they do not become actual dangers to customers or for employees.  **e-Safety Risks and Issues**  e-Safety risks and issues can be generally classified into three areas: content, contact and commerce. The following are basic examples of the types of e-Safety risk and issues that could fall under each category.  **Content:**   * Exposure to inaccurate or misleading information * Exposure to socially unacceptable material such as that inciting violence, hate or intolerance * Exposure to illegal material, such as promotion of terrorism and images of child abuse * Exposure to risks associated with radicalisation and extremism, including violent extremist literature that lead to terrorist-related activity * Exposure to age-inappropriate material * Downloading of copyrighted materials, e.g. music and films * Use of remarks, ‘jokes’ and banter in electronic communications or social media, about age, disability, gender, race, religion or belief or sexual orientation, gender re-assignment which are offensive, abusive or belittling and detrimental to a good working environment * Plagiarism   **Contact:**   * Grooming using ICT, leading to sexual assault and/or child sexual exploitation * Bullies using ICT (email, mobile phones, chat rooms, social media etc) as a way to torment their victims, known as cyber bullying) * People self-publishing information-sometimes inappropriate about themselves and therefore putting themselves at risk   **Commerce:**   * Exposure to inappropriate commercial advertising * Exposure to online gambling services * Phishing * Commercial and financial scams   **The aim of this e-Safety Policy is to:**   * To raise e-safety awareness and the use of internet safety measures amongst staff and customers to safeguard them from possible harm * To ensure that Managers and staff champion the e-Safety agenda and that this strategy is fully endorsed at all levels * To focus on opportunities for safe learning using a wide range of technology including social networking, whilst building resilience as well as reducing risk * To be informed of latest developments in terms of the gaps in our knowledge around digital safety * Ensure that we target the needs of specific groups, such as vulnerable adults at risk and young people * Promote the availability and use of digital controls and monitoring software * To highlight the increased functionality of mobile phones, games consoles and other new technology * To look at internet use and the risks faced by young people and adults and ensure that e-Safety learning is promoted, to provide a firm foundation for a targeted preventative approach * To provide policy, guidance and support including responsible use of technology. * To raise customer awareness of cyber bullying, and of potential threats of radicalisation and extremism and what to do if these instances arise * To ensure that staff recognise the importance of ensuring that customers understand the do’s and don’ts of safe use of technology * We are committed to the principle of e-Safety across all our provision through the use of monitoring and training to raise awareness for both staff and customers * To ensure that public awareness campaign messages are coordinated and embedded in support materials for managers and staff teams * Signposting customers to access further help and support * Include information for customers about e-Safety when they are away from Skills for Work e.g. at home or on placement.   Procedure   * E-Safety concerns: Every e-safety concern will be assessed in relation to Safeguarding. * All e-Safety concerns/incidents will be recorded as part of Skills for Work Safeguarding process and procedure and adhere to BMDC policy and guidelines and * All staff will ensure that any e-Safety concerns are reported and will assist where possible with any follow up. * Ensuring risk assessments where required and recognise that e-safety issues must often present a Safeguarding risk * The designated safeguarding lead will be responsible for ensuring all e-safety issues that pose a Safeguarding risk are investigated * Organise timely and appropriate staff training in relation to e-safety issues as part of Skills for Work’s safeguarding training * All staff are responsible for ensuring that: They have read and understood Bradford Council’s [Your Council Information Security Policy (bradford.gov.uk)](http://intranet.bradford.gov.uk/your-council/policies-and-protocols/information-security-policy)   + They report any suspected misuse or problems through the appropriate channels Skills for Work Safeguarding process / Bradford Councils   + Teaching subject matter that communicates and reinforces the importance of e-safety, with special regard for safeguarding issues * All Learners are responsible for ensuring that they understand the importance of reporting abuse, misuse or access to inappropriate materials   Skills for Work will remove, block, ban and, if necessary, report users to the associated media platforms who violate acceptable norms with direct messages that:   * Bully, harass or intimidate * Are unlawful, libellous, defamatory, abusive, threatening, harmful, obscene, profane, sexually orientated or racially abusing. * Infringe the or violate someone else’s rights * Violate or intellectual property rights * Advertise products or services   Skills for Work will also ban any users who:   * Encourage others to post such messages * Use offensive imagines as their profile picture * Have an offensive username   The following policy should be read in conjunction with Bradford Council’s policies and mandatory training for staff:  Safeguarding  Protecting Information e-learning  [Your Council Information Security Policy (bradford.gov.uk)](http://intranet.bradford.gov.uk/your-council/policies-and-protocols/information-security-policy)  All information and guidance for users including e-safety, safeguarding, health and safety and complaints process will be included in user/learner Welcome booklet issued to all users and staff. Welcome/Induction booklet is also available via Skills for Work (insert link) and hard copies will be available on request.  Reviewed: 27th February 2024 Reviewer: Suzan Mc Gladdery  **e-Safety Incident Reporting Flowchart**  Observed incident  Accidental or Intentional?  **Accidental**  **Intentional**  Note website concerned and nature of content  Note nature of incident e.g. cyberbullying, intentional attempt to access prohibited material etc.  Remove image/content from screen and reassure learner (including others who may have witnessed the event)  Preserve evidence.  (take a screen shot by pressing alt & print screen and copying onto word document)  Report website to helpdesk (1234) or authorised person for blocking  Notify Skills for Work Designated Safeguarding Officer  Apply disciplinary sanctions as appropriate  Notify Skills for Work Designated Safeguarding Officer |