E-Safety Policy

V3.0 / QU018

1. Our Commitment

1.1 The Childcare Company / Impact Futures are committed to ensuring the safety and well-being of all our learners. As apprenticeship delivery continues to evolve and becomes even more inclusive of a blended learning model with the use of technology in learning. It is our responsibility to ensure our learners understand how to protect themselves against online threats and effectively recognise unethical behaviours.

1.2 Our approach is to implement safeguards to support learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. In furtherance of our duty to safeguard vulnerable people, we will do all that we can to make our learners stay 'e-safe' and to satisfy our wider duty of care.

2. Statement of Purpose

2.1 This policy outlines the responsibilities that we expect from all learners whilst undertaking their chosen apprenticeship with The Childcare Company / Impact Futures.

3. Policy Aims

3.1 We aim to make this policy easy to understand and access.

3.2 We will provide additional IT support and guidance to any learner that encounters issues with accessing The Childcare Company / Impact Futures apprenticeship systems.

3.3 We aim to provide learning opportunities to support learners to understand their responsibilities and protective measures against online threats and unethical behaviours.

3.4 We aim to encourage the use of safe behaviours during teaching and 121 sessions.

4. Scope

4.1 The policy applies to all learners who have access to IT systems. Any learner of IT systems must adhere to E-Safety rules.

4.2 The E-Safety Policy applies to all use of the internet, and electronic communication devices such as email, mobile phones, games consoles, social networking sites, and any other systems that use the internet for connection and providing of information.

5. Aims

The aims are to:

5.1 To ensure safeguards on IT-based systems are strong and reliable.

5.2 To ensure user behaviour is safe and appropriate.

5.3 To assure that the storage and use of images and personal information on IT based systems is secure and meets all legal requirements.

5.4 To educate learners in e-safety

5.5 To ensure any incidents which threaten e-safety are managed appropriately.

6. Definition of E-Safety

6.1 The term e-safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures, and education, including training, underpinned by standards and inspection.

6.2 E-safety risks can be summarised under the following three headings:

Content

a) Exposure to age-inappropriate material

b) Exposure to inaccurate or misleading information

c) Exposure to socially unacceptable material, such as that inciting violence, hate, extremism, or intolerance

d) Exposure to illegal material, such as images of child abuse

e) Illegal Downloading of copyrighted materials e.g. music and films

Contact

a) Grooming using communication technologies, potentially leading to sexual assault or child

b) Prostitution

c) Radicalisation - the process by which a person comes to support terrorism and extremist

d) Ideologies associated with terrorist groups.

e) Bullying via websites, mobile phones or other forms of communication device

Commerce

a) Exposure of minors to inappropriate commercial advertising

b) Exposure to online gambling services

c) Commercial and financial scams

7. Behaviour

7.1 You will not reveal your passwords to anyone or keep a record of your passwords which can be easily accessed and understood by another person.

7.2 If your password is compromised, you will ensure you change it or contact your Development Coach.

7.3 You will not use anyone else's password.

7.4 You will not allow unauthorised people to access your Email, Aptem, Smart Assessor, BKSB or any other account that is created for your Apprenticeship.

7.5 You will not engage in any online activity that may affect your learning opportunities e.g., using other people's work as your own.

7.6 You will only use approved, secure email systems and mobile devices to contact your Development Coach in relation to your apprenticeship.

7.7 You will only use Teams/Zoom account to contact your Development Coach and to attend teaching & learning sessions.

7.8 When using Teams/Zoom, you will always look presentable to conduct meetings with your Development Coach or any other individual that is involved within your apprenticeship.

7.9 You will attend your apprenticeship appointments in a calm and quiet environment.

7.10 You will not browse, download, or send material that could be considered offensive.

7.11 When undertaking research activities for your apprenticeship you will ensure that websites used are safe and secure. In addition, you will not click on any website link you feel is not secure. If unsure, please contact your Development Coach.

7.12 You will not publish or distribute work that is protected by copyright.

7.13 You are encouraged to install anti-virus software on your devices and maintain its protection.

7.14 If you feel that your Email address has been compromised, you will report this to your Development Coach.

8. Use of images and video

8.0 The use of images or photographs is encouraged in teaching and learning. Providing there is no breach of copyright or other rights of another person.

8.1 Learners are trained in the risks in downloading, posting, and sharing images, and particularly in the risks involved in posting personal images onto social networking sites, for example.

8.2 Advice and approval from your Development Coach is sought in specified circumstances or if there is any doubt about the publication of any materials.

9. Education and Training

9.0 Learners are supported through training and education to develop the skills to be able to identify risks independently and manage them effectively.

9.1 Learner inductions and the tutorial programme contains sessions on e-safety.

9.3 Learners are guided in e-safety across the curriculum and opportunities are taken to reinforce e-safety messages.

9.2 Learners know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

9.3 Learners are encouraged to question the validity and reliability of materials researched, viewed, or downloaded. They are encouraged to respect the copyright of other parties and to cite references properly.

10. Legal and other Frameworks

10.0 Working together to safeguard children (HM Government) July 2018

10.1 Keeping children safe in education (DfE) September 2023

10.2 The Prevent Duty (HM Government) June 2015

10.3 Channel Duty Guidance (HM Government) (2020)

10.4 Inspecting safeguarding in early years, education, and skills settings (Ofsted) 2 September 2019

10.5 The Education (Independent School Standards) Regulations (2014)

10.6 The Equality Act (2010)

10.7 The Human Rights Act 1998

10.8 Searching, screening and confiscation in schools (January 2018)

10.10 Sexting in Schools and Colleges (UK Council for Child Internet Safety)

11. Declaration

11.0 The Childcare Company/Impact Futures require you to have read this policy and to sign to confirm that you understand your responsibilities as outlined in bullets 7.1 – 7.14.

(a) I agree to abide by all the points above.

(b) If you have any concerns at any time regarding digital technologies, passwords or GDPR, please contact your Development Coach.

Learner Signature:	
Print Name:	
Date Signed:	

12. Context

12.0 This policy has been developed in accordance with the Learner Handbook.

13. Appendices

13.1 Appendix 1:

a) QU011 Learner Handbook Policy – Procedures

14. Document control

Document Reference	QU018
Document Title	E-Safety Policy V3.0
Version	3
Original Author	Deanne Stubbs-Ambrose / Samantha Johnson
Authors Title	Quality Manager
Policy Owner	Nicole Smith
Original Issue	July 2022
Review Date	October 2023
Author of Revision	Joanne Wilson
Date of Revision	October 2023
Revision Number	3
Reason for Revision	Policy Update
Amendments	7.4 Addition of Aptem 10.1 Update to 2023 version

Signed

Printed Name Nicole Smith

Job Title Chief Operating Officer

Date 6th October 2023