

Online and E-Learning Policy

Skills Bootcamp Provision | Adult Learners 19+ | Version 2.0

Policy field	Current position
Provider	Quack Recruitment & Training Ltd
Applies to	Adult learners aged 19+, staff, tutors, assessors, progression staff, managers, employers and any authorised user of Quack digital learning systems
Policy owner	Jessica Roughton – Quality & Compliance Lead, DSL and SEND Lead
Senior accountable lead	Dion Bishop – Director of Contracts & Operations
Designated Safeguarding Lead	Jessica Roughton
Deputy Designated Safeguarding Lead	Aaron Jones
Approved systems	Microsoft Teams, PICS, BKSB, Highfield Vault / Highfield systems, approved email and approved learner communication channels
Next review	June 2027 or sooner following legislative, safeguarding, data protection, funder, awarding body or operational change

Policy intent: Online learning must be safe, inclusive, well managed, professionally delivered and auditable. This policy sets out the controls used by Quack Recruitment & Training Ltd to protect learners, staff and personal information while ensuring online learning contributes to learner progress, safeguarding, inclusion, achievement and progression.

Contents

1. Purpose and Policy Intent.....	3
2. Scope and Application	3
3. Legal, Regulatory and Inspection Context	3
4. Definitions	4
5. Policy Statement.....	4
6. Approved Platforms and Communication Channels.....	5
7. Digital Readiness, Access and Induction	5
8. Attendance, Participation and Engagement	6
9. Online Classroom Conduct and Professional Standards	6
10. Cameras, Microphones, Chat, Breakout Rooms and Recordings	7
11. Safeguarding, Prevent and Online Safety	7
12. Inclusion, SEND and Reasonable Adjustments	8
13. Data Protection, Confidentiality and Information Security	8
14. Assessment, Academic Integrity and Artificial Intelligence	9
15. Learning Resources, Images, Recordings and Copyright.....	9
16. Roles and Responsibilities	10
17. Reporting Concerns, Breaches and Incidents	10
18. Monitoring, Quality Assurance and Review.....	11
Appendix A: Online Session Readiness Checklist	12
Appendix B: Learner Online Conduct Checklist	12
Appendix D: Version Control	13

1. Purpose and Policy Intent

Quack Recruitment & Training Ltd is committed to providing online and blended learning that is safe, inclusive, accessible, professionally delivered and effective in supporting learner progress. This policy defines the standards and controls that apply to online learning, remote classroom delivery, e-learning activity, digital assessment preparation, learner communication and use of approved learning systems.

The purpose of this policy is to ensure that learners can participate in online learning safely and confidently, that staff understand their responsibilities, and that leaders can evidence effective oversight of safeguarding, Prevent, online safety, data protection, learner engagement, inclusion, assessment integrity and quality assurance.

This policy replaces the previous Online E-Learning Policy Version 1.0 and strengthens the document by adding clearer controls for adult Skills Bootcamp delivery, safeguarding, Prevent, digital readiness, AI use, assessment integrity, incident reporting, monitoring and Ofsted readiness.

2. Scope and Application

This policy applies to all online learning and digital communication connected to Quack Recruitment & Training Ltd provision. This includes fully online delivery, blended delivery, online-supported learning, remote learner support, digital assessment preparation and employer-linked online activity.

Applies to	Examples
Learners	Adult learners aged 19+ enrolled on Skills Bootcamp provision, including remote, classroom-based and blended learners.
Staff	Tutors, assessors, IQAs, progression officers, learner engagement staff, managers, quality/compliance staff and senior leaders.
Employers and external contributors	Employer partners, guest contributors or interviewers participating in online activity, where applicable.
Digital systems	Microsoft Teams, PICS, BKSB, Highfield Vault / Highfield systems, approved email and any other approved platform.
Learning activities	Live teaching, recorded or shared learning resources, learner reviews, online meetings, tutorials, assessment preparation, learner support, employer preparation and progression activity.

The policy applies whether learners use a Quack-managed device, their own device, employer equipment or another approved learning device. Where learners cannot meet digital access expectations, staff must consider support options, reasonable adjustments or alternative arrangements where appropriate.

3. Legal, Regulatory and Inspection Context

This policy is informed by the following legal, regulatory and inspection expectations. It should be read alongside the provider's Safeguarding Policy, Prevent Risk Assessment, Information Security Policy, GDPR and Privacy Policy, Learner Support Policy, Equality, Diversity and Inclusion Policy, Malpractice and Maladministration Policy, Assessment/IQA arrangements and learner handbook.

Framework	Relevance to online learning
UK GDPR and Data Protection Act 2018	Requires personal information to be processed lawfully, fairly, securely and only for appropriate purposes.
Counter-Terrorism and Security Act 2015 and Prevent Duty guidance	Requires providers to have due regard to preventing people from being drawn into terrorism and to treat radicalisation risk as a safeguarding matter.
Safeguarding adults principles and local safeguarding arrangements	Online learning controls must support the identification, reporting and escalation of learner welfare and safeguarding concerns.
Equality Act 2010	Requires reasonable adjustments and inclusive access for disabled learners and learners with support needs.
Ofsted further education and skills inspection materials	Inspectors consider safeguarding, inclusion, leadership, curriculum, achievement, participation and learner development, including how leaders know learners are safe and supported.
Awarding body and funder requirements	Online delivery and assessment-related activity must meet qualification, audit, evidence and funding rules.

4. Definitions

Term	Meaning for this policy
Online learning	Live or supported learning delivered through digital platforms such as Microsoft Teams, PICS, BKSB or Highfield systems.
Blended learning	A programme that includes both face-to-face and online or digitally supported learning activity.
Approved platform	A system approved by Quack Recruitment & Training Ltd for delivery, learner support, assessment preparation, communication or evidence collection.
Official communication channel	A company-approved email, Teams channel, PICS record or other authorised channel used for learner communication.
Safeguarding concern	Any concern about learner safety, welfare, abuse, exploitation, radicalisation, harassment, self-harm risk, online risk or vulnerability.
Data breach	A security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
AI tool	Any generative or assistive technology that can produce or substantially amend text, answers, images, code, plans, summaries or learner work.

5. Policy Statement

Quack Recruitment & Training Ltd will ensure that online learning is planned, monitored and delivered in a way that protects learners, supports progress and maintains professional standards. Online learning must be purposeful, accessible, secure and aligned to the same safeguarding, inclusion, teaching, assessment and quality expectations as classroom-based delivery.

The provider will maintain clear rules for attendance, participation, online conduct, use of approved systems, data protection, safeguarding, Prevent, learner support and reporting concerns. Staff are expected to use online platforms professionally and to remain alert to learner engagement, welfare, inclusion, assessment and progression risks.

The impact intended by this policy is that learners can participate safely, understand online expectations, access support where needed, engage with learning, protect their personal information and use digital systems

appropriately. Leaders will use learner feedback, attendance records, safeguarding records, quality assurance activity, staff feedback and system evidence to monitor whether online learning is safe, inclusive and effective.

6. Approved Platforms and Communication Channels

Only approved systems and communication channels may be used for delivery, learner support, learner review, assessment preparation, progression activity and exchange of learner information. Staff must not use personal social media accounts, personal messaging apps or unauthorised platforms to communicate with learners about provision.

Platform / channel	Approved use	Control expectation
Microsoft Teams	Live teaching, learner reviews, remote meetings, staff meetings and employer-related online activity.	Tutors monitor attendance, chat, conduct, engagement and safeguarding indicators.
PICS	Learner management, IAG, attendance, contact notes, learner records, ILPs, support records and progression evidence.	Records must be accurate, timely and kept up to date.
BKSB	English and mathematics initial assessment and learning activity.	Results and progress are used to inform support and learner review.
Highfield Vault / Highfield systems	Qualification evidence, assessment-related activity and awarding body processes where applicable.	Used in line with awarding body requirements, malpractice controls and evidence standards.
Approved email	Formal communication with learners, staff, employers, funders and awarding bodies.	Personal data must be shared securely and only with appropriate recipients.

New software, systems or online tools must not be introduced for learner-facing activity without management approval and consideration of safeguarding, data protection, accessibility, information security, record retention and quality assurance risks.

7. Digital Readiness, Access and Induction

Digital readiness must be considered before and during delivery. Enrolment and IAG activity should identify whether learners have suitable equipment, internet access, email access, a quiet learning environment, confidence using online systems and any barriers that may affect participation.

- Learners should receive clear joining instructions before online sessions, including time, platform, link, expected conduct, attendance requirements and support contact route.
- Tutors must confirm learners know how to access the session, use basic platform functions and raise technical or safeguarding concerns.
- Learners who experience digital barriers should be supported through practical guidance, reasonable adjustments or alternative arrangements where appropriate.
- Online learning expectations should be reinforced during induction, learner handbook review, early delivery and learner review activity.
- Learners should be reminded that online participation forms part of their attendance, engagement and professional behaviour record.

8. Attendance, Participation and Engagement

Attendance and engagement in online learning are treated as employability behaviours as well as funding, quality and learner-progress controls. Learners are expected to attend online sessions punctually, participate appropriately and notify staff promptly where they cannot attend.

Area	Expectation	Evidence / monitoring
Attendance	Learners attend on time and remain present for the full planned session unless agreed otherwise.	Teams attendance, registers, PICS attendance record and tutor follow-up.
Absence reporting	Learners report absence before 9.00am or before the planned start time where sessions begin earlier.	Absence notes, PICS contact record and attendance intervention evidence.
Engagement	Learners participate through discussion, chat, activities, questions, tasks, assessment preparation and learner review.	Tutor observation, ILP review, skills scans, learner voice and work completion.
Non-attendance follow-up	Staff follow up non-attendance promptly and consider whether there are barriers, welfare or safeguarding concerns.	PICS contact notes, safeguarding records where relevant and learner support actions.

Where learners repeatedly fail to attend or engage, staff must identify whether the issue relates to poor engagement, digital barriers, employment, caring responsibilities, health, confidence, safeguarding, welfare, SEND, English or mathematics needs, or another barrier requiring support.

Tutors must take reasonable steps to confirm learner identity, attendance and engagement during online sessions. This may include checking the learner's name on the platform, confirming presence verbally or through chat, monitoring participation, recording attendance accurately and following up where there is doubt about identity, attendance, engagement or completion of planned learning activity.

9. Online Classroom Conduct and Professional Standards

Online sessions must reflect the same standards of behaviour and professionalism expected in face-to-face learning and future employment. Learners and staff must behave respectfully, maintain professional boundaries and use appropriate language at all times.

Expected behaviour	Not acceptable
Arrive on time, prepared and appropriately dressed.	Disruptive behaviour, repeated lateness or disengagement without explanation.
Use appropriate language and professional communication.	Abusive, discriminatory, sexualised, extremist, threatening or harassing comments.
Respect tutor instructions for microphones, cameras, chat and activities.	Ignoring tutor directions, misusing chat or interrupting learning.
Use suitable backgrounds and surroundings.	Inappropriate images, offensive material, unsafe environments or distracting settings.
Respect confidentiality and privacy of other learners.	Screenshots, recordings or sharing learner information without approval.

Breaches of online conduct may result in removal from the online session, learner support intervention, disciplinary action, safeguarding referral, awarding body notification or external agency referral depending on seriousness.

10. Cameras, Microphones, Chat, Breakout Rooms and Recordings

Tutors must set clear expectations for cameras, microphones, chat, breakout rooms and recording at the start of online delivery. Controls should support engagement and safeguarding while also recognising accessibility, confidence, privacy and reasonable adjustment needs.

Feature	Policy expectation	Safeguarding / quality control
Cameras	Learners are expected to use cameras where appropriate unless a reasonable adjustment, privacy issue or agreed support need applies.	Tutors monitor presence, engagement and welfare indicators proportionately.
Microphones	Learners should use microphones appropriately and mute when not speaking to reduce disruption.	Tutors manage discussion to support participation and respectful communication.
Chat	Chat must be used for learning, questions and tutor-approved communication only.	Tutors monitor chat and report inappropriate, discriminatory or safeguarding-related content.
Breakout rooms	Breakout rooms may be used only where planned, supervised and appropriate for the activity.	Tutors must retain oversight and ensure learners know how to request help.
Recordings	Learners and staff must not record sessions unless recording has been explicitly authorised by management and all relevant controls are in place.	Unauthorised recording is treated as a serious breach of policy and may be escalated.

Where a session recording is authorised for accessibility, quality assurance or delivery reasons, leaders must consider lawful basis, consent or notification requirements, storage location, retention period, access controls, safeguarding risk and whether recording could capture sensitive personal data.

Learners' privacy must be respected during online learning. Staff should not ask learners to show private areas of their home or personal environment unless this is necessary for a legitimate safeguarding, identity, assessment or learning reason. Learners may use appropriate blurred or neutral backgrounds where this supports privacy, dignity or reasonable adjustment, provided engagement and safeguarding expectations can still be met.

11. Safeguarding, Prevent and Online Safety

Safeguarding responsibilities apply fully to online learning environments. Staff must remain alert to signs of learner distress, disengagement, radicalisation risk, cyberbullying, online harassment, exploitation, grooming, domestic abuse, financial vulnerability, mental health concerns, inappropriate sharing of images or information, and unsafe online behaviour.

Online risk	Examples	Control response
Harmful content	Extremist material, self-harm content, misinformation, hate content, sexualised content or illegal content.	Tutor monitoring, learner reporting routes, Prevent training and DSL escalation.
Cyberbullying / harassment	Abusive chat, targeted comments, intimidation, discrimination or victimisation.	Immediate tutor intervention, recording, learner support and disciplinary/safeguarding escalation.
Radicalisation / Prevent concern	Extreme views, support for violence, fixation on grievance, sharing extremist content or vulnerability to extremist narratives.	Report to DSL/DDSL immediately and follow Prevent/safeguarding procedures.
Grooming / exploitation	Manipulative contact, pressure to share images, financial exploitation or unsafe relationships.	Safeguarding report, learner support and external referral where required.
Online disengagement as welfare indicator	Sudden withdrawal, camera avoidance, repeated absence, distress, changes in	Attendance follow-up, welfare check, support discussion and safeguarding

Online risk	Examples	Control response
	communication or behaviour.	consideration.

All safeguarding, Prevent or welfare concerns identified during online learning must be reported immediately to the DSL or Deputy DSL using the provider's safeguarding reporting procedure. Staff must not investigate concerns themselves, promise confidentiality or delay escalation where risk is present.

Learners must be reminded during induction and delivery how to raise online safety, safeguarding or Prevent concerns. Reporting routes must be visible through learner handbooks, onboarding information, Teams prompts, staff communication and learner review activity.

12. Inclusion, SEND and Reasonable Adjustments

Online learning must be inclusive and accessible. Leaders recognise that learners may experience barriers linked to digital confidence, English and mathematics, SEND, anxiety, mental health, disability, home environment, caring responsibilities, internet access, equipment, confidence or previous negative experiences of education.

- Learners should be asked during IAG whether they have the equipment, internet access and environment needed to participate online.
- Tutors should use PICS, IAG, BKSb, skills scans, ILP reviews and tutor handover information to understand support needs before and during delivery.
- Reasonable adjustments may include additional explanation, adapted resources, changed background colours, extra time, digital support, alternative communication, additional check-ins, quieter participation options or assessment preparation support.
- Where learners do not disclose a support need at enrolment, tutors should remain alert to emerging needs through engagement, written work, confidence, attendance, assessment performance and learner discussion.
- Support actions should be recorded and reviewed so leaders can evidence the impact of support on participation, progress and achievement.

The intended impact is that learners are not excluded from online learning because of digital, confidence, SEND, wellbeing or accessibility barriers. Leaders will monitor this through learner voice, attendance, ILP reviews, support records, quality assurance activity and learner file review.

13. Data Protection, Confidentiality and Information Security

All users must protect personal data, learner records, assessment information, safeguarding information and company systems. Staff must comply with UK GDPR, the Data Protection Act 2018, the provider's GDPR and Privacy Policy and Information Security Policy.

All users must	All users must not
Use strong passwords and keep passwords confidential.	Share login credentials.
Lock devices when unattended.	Access another user's account without authorisation.
Use approved systems and official communication channels.	Download or store learner information on personal devices without approval.
Report suspected data breaches, phishing, malware or unauthorised access immediately.	Share learner information through personal email or social media.
Check recipients before sending learner or staff information.	Leave devices or learner records visible to unauthorised people.
Store files only in approved secure locations.	Upload malicious software or attempt to bypass security controls.

Suspected personal data breaches must be reported immediately to management so the provider can assess risk, contain the incident, record the breach and decide whether notification to affected individuals, funders, awarding bodies or the Information Commissioner's Office is required.

14. Assessment, Academic Integrity and Artificial Intelligence

Online learning and digital systems may be used to support assessment preparation, portfolio development, learner reflection, formative checks and qualification-related activity where permitted by the awarding body and programme requirements. Assessment integrity must be maintained at all times.

Learners may use AI tools only where the tutor has authorised their use for learning support, idea development, practice, explanation or accessibility purposes. Learners must not submit AI-generated work, copied work or work produced by another person as their own. Any submitted work must represent the learner's own understanding and meet awarding body requirements.

Area	Permitted where authorised	Not permitted
AI support	Using AI to explain a concept, practise questions, generate revision prompts or support understanding.	Submitting AI-generated answers as the learner's own assessment evidence.
Assessment work	Using approved resources and tutor guidance to prepare for assessment.	Copying from AI, websites, other learners or unauthorised sources.
Evidence of understanding	Learners may be asked to explain work verbally or through discussion to confirm understanding.	Refusing or being unable to explain submitted work where authenticity is in doubt.
Tutor/IQA checks	Tutors and IQA may review work for authenticity, consistency and learner understanding.	Using tools to bypass assessment, mislead staff or falsify evidence.

Suspected misuse of AI, plagiarism or unauthorised assistance may be investigated under the provider's Malpractice and Maladministration Policy and reported to the awarding body where required.

15. Learning Resources, Images, Recordings and Copyright

Learning resources shared through online learning remain the intellectual property of the provider, awarding body, tutor, employer or original copyright holder as applicable. Learners and staff must not publish, distribute or upload learning materials externally without authorisation.

- Learners must not record, screenshot or photograph sessions, learners, staff, slides, chat, assessment materials or learner information unless explicit permission has been given.
- Staff must not share learner images, recordings or personal information without a lawful basis, permission where required and approval from management.
- Learning resources may be emailed or uploaded to approved systems where this supports learner progress and does not breach copyright, awarding body rules or data protection requirements.
- Any use of images or recording for evidence, marketing, learner support, accessibility or quality assurance must be controlled, stored securely and reviewed against safeguarding and data protection requirements.

16. Roles and Responsibilities

Role	Key responsibilities	Evidence / assurance
Director of Contracts & Operations	Senior accountability for policy implementation, resources, contract compliance, quality oversight and escalation of serious incidents.	Leadership review, QIP, contract monitoring and incident escalation records.
Quality & Compliance Lead / DSL / SEND Lead	Owns policy review, safeguarding oversight, online safety monitoring, SEND access, reasonable adjustments, quality assurance and staff guidance.	Policy review, safeguarding records, learner support records, QA activity and staff communication.
Deputy DSL / Lead Assessor	Supports safeguarding escalation, assessment integrity, tutor practice, learner progress, online conduct and quality of assessment evidence.	Safeguarding notes, assessment review, IQA/standardisation and tutor support.
Tutors / Assessors	Deliver safe and effective online learning, monitor attendance and engagement, maintain professional boundaries, record concerns and support learner progress.	Registers, PICS notes, ILPs, learner work, skills scans, feedback and safeguarding referrals.
Learner Engagement / Progression Staff	Support learners with access, engagement, attendance, employability, job matching, employer contact and progression evidence.	PICS notes, progression records, employer evidence and learner contact logs.
IT Support / Approved technical support	Maintain secure systems, manage access, support technical issues and respond to security incidents as required.	Access logs, support records, incident records and system updates.
Learners	Attend, participate, behave professionally, protect accounts, respect others, report concerns and complete work honestly.	Attendance, learner voice, ILPs, conduct records and assessment evidence.

17. Reporting Concerns, Breaches and Incidents

Any learner, staff member, employer or authorised user who witnesses or experiences online safety concerns, cyberbullying, harassment, discrimination, inappropriate behaviour, safeguarding concerns, Prevent concerns, data breaches, security incidents, assessment malpractice or misuse of systems must report the matter promptly.

Incident type	Immediate action	Record	Escalation
Safeguarding / welfare concern	Ensure immediate safety where possible and report to DSL/DDSL without delay.	Safeguarding concern form/log and PICS where appropriate.	DSL/DDSL, external agency where required.
Prevent concern	Do not investigate. Report to DSL/DDSL immediately.	Safeguarding/Prevent log.	DSL/DDSL, Channel/local Prevent/police where required.
Online conduct breach	Tutor intervenes, stops behaviour and removes learner from session if necessary.	PICS note, conduct record, learner support/disciplinary record.	Manager/DSL/awarding body where relevant.
Data breach / security incident	Contain if possible, preserve evidence and report to management immediately.	Data breach/security incident log.	Senior lead, ICO/funder/awarding body where required.
Assessment malpractice / AI misuse	Secure evidence and do not make unsupported accusations.	Malpractice record and assessment/IQA evidence.	Quality lead/IQA/awarding body where required.

Failure to comply with this policy may lead to learner disciplinary action, removal from online sessions, suspension from learning activity, awarding body referral, staff disciplinary action, contract escalation or referral to external agencies depending on severity.

18. Monitoring, Quality Assurance and Review

Leaders will monitor the effectiveness of this policy through quality assurance, learner records, staff feedback, learner voice, safeguarding review, data protection monitoring and QIP review. The policy will be reviewed annually, or sooner where there is a safeguarding, legal, data protection, funder, awarding body, system or operational change.

Monitoring activity	Purpose	Frequency / trigger
Learner voice / reviews	Check whether learners feel safe, supported, able to access systems and clear about expectations.	Mid-point, endpoint and as required.
Attendance and engagement review	Identify disengagement, digital barriers, welfare concerns and support needs.	Daily/weekly during delivery.
OTLA / QA activity	Evaluate quality of online teaching, engagement, inclusion, safeguarding prompts and learner progress.	Planned QA cycle and as required.
Learner file review	Check records show IAG, digital readiness, support, attendance, ILP, assessment and progression evidence.	Planned sampling and QIP review.
Safeguarding / Prevent review	Check concerns, trends, learner awareness and staff confidence.	Ongoing, with formal review as part of safeguarding oversight.
Staff feedback / CPD review	Identify staff training, workload, system and confidence needs.	Staff surveys, meetings and CPD reviews.
Information security review	Monitor data protection, access control and system risks.	Ongoing and following incidents.

The policy owner will ensure that review findings are used to update guidance, staff CPD, learner induction, QIP actions, system controls and risk assessments where required.

Appendix A: Online Session Readiness Checklist

Stage	Check	Complete / evidence
Before session	Teams link, timetable and joining instructions sent to learners.	
Before session	Tutor has register, learner list, support notes and any reasonable adjustments.	
Before session	Learning resources are ready and stored in approved location.	
Before session	Safeguarding/Prevent/reporting route reminder is available for display or verbal reinforcement.	
Start of session	Attendance, cameras/mics/chat expectations and conduct standards are reinforced.	
During session	Tutor monitors attendance, engagement, chat, welfare indicators and understanding.	
During session	Learners who need support receive prompts, alternative explanations or follow-up.	
End of session	Next steps, tasks, assessment preparation and support routes are clarified.	
After session	Register, PICS notes, concerns, ILP updates or support actions are completed.	

Appendix B: Learner Online Conduct Checklist

- I will attend online sessions on time and notify staff promptly if I cannot attend.
- I will participate respectfully and use appropriate language at all times.
- I will use approved systems and official communication channels only.
- I will not record, screenshot or share online sessions, resources, chat or learner information without permission.
- I will protect my login details and not share passwords or access another person's account.
- I will report safeguarding, online safety, cyberbullying, harassment, Prevent or data security concerns promptly.
- I understand that assessment work must be my own and that misuse of AI, copying or plagiarism may be treated as malpractice.
- I understand that online behaviour, attendance and engagement are part of my learner record and employability development.

Appendix D: Version Control

Version	Date	Author / owner	Summary of change	Approved by	Next review
1.0	June 2026	Quack Recruitment & Training Ltd	Initial Online E-Learning Policy produced.	Senior Leadership Team	February 2027

Reference framework: This policy should be read alongside the provider's safeguarding, Prevent, data protection, information security, learner support, EDI, assessment, malpractice, learner conduct and quality assurance documentation.

External reference sources considered: statutory Prevent Duty guidance, DfE Prevent resources for education, ICO UK GDPR guidance/resources, and Ofsted further education and skills inspection materials.