

QA Learning Code of Conduct

Prepared by: Sohail Oosman

Prepared for: QA Group

Date: 08 June 2026

Issue: 1

PUBLIC

This document can be disclosed outside of the QA group of companies.

Version control

Document information	
Version 1	New document

Document Approval		
Name	Position	Viewed / comments
Tamryn Fischer	Paralegal	Approved
Clare Dunne	Head of Quality	Approved
Sohail Oosman	Director of Learning	Approved
David Black	Information Security & Compliance Manager	Approved

Revision History			
Version	Issue date	Author	Description of change
1	14/05/2026	Sohail Oosman/Clare Dunne/ Tamryn Fischer / David Black	New document

Contents

1. Introduction	3
1.1. Overview	3
1.2. Scope	3
1.3. Core Principles	3
2. Legal and Data Protection Notice	4
3. Monitoring and Security	4
4. Use of Training Environments and Technology	5
4.1. General Use	5
4.2. Prohibited Activities	5
4.3. Acceptable Use of Assets	5
4.4. Intellectual Property	6
4.5. Recording of Training Sessions	6
4.6. Use of Artificial Intelligence (AI)	7
4.7. Use of External Platforms	8
5. Confidentiality and Professional Conduct	8
5.1. Confidentiality	8
5.2. Professional Conduct	8
5.3. Use of Corporate Devices	9
6. Online Safety and Behaviour	9
7. Compliance and Enforcement	9
7.1. Reporting	9
7.2. Non-Compliance	10
7.3. Enforcement	10
7.4. Liability	10
8. Review and Maintenance	10
Schedule A: Recording Guidelines	11



1. Introduction

1.1. Overview

This Code of Conduct defines the standards expected of all learners participating in QA training, whether delivered in-person or virtually.

It exists to:

- Safeguard the confidentiality, integrity, and availability of information;
- Protect learners, staff, and third-party interests;
- Ensure compliance with legal, regulatory, and contractual obligations.

This Code aligns with:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- ISO/IEC 27001 information security principles

1.2. Scope

This Code applies to:

- All learners attending commercial QA training
- All QA learning environments (physical and virtual)
- All systems, platforms, and materials provided or used during training

1.3. Core Principles

Learners must:

- Act with integrity and professionalism
- Respect confidentiality and privacy
- Protect intellectual property



- Use technology responsibly and transparently

Training sessions, materials and interactions must not be recorded, captured or shared unless explicitly authorised.

2. Legal and Data Protection Notice

QA processes personal data in accordance with UK GDPR.

Learners must:

- Access personal data only when authorised
- Not record, store or share personal data unless authorised and legally permitted
- Maintain confidentiality of all participants

Unauthorised handling of personal data may:

- Breach legal obligations
- Result in sanctions
- Give rise to personal liability

Learners must immediately report any suspected data breach or unauthorised disclosure.

3. Monitoring and Security

QA may monitor access to systems and learning platforms for:

- Security and threat detection
- Compliance monitoring
- Service quality and improvement
- Proportionate monitoring in line with data protection requirements

Learners must not:

- Attempt to bypass or interfere with monitoring controls



- Use tools or techniques to conceal activity

Learners are responsible for:

- Maintaining the confidentiality of login credentials
- Logging out of shared or public systems
- Reporting suspected account compromise

4. Use of Training Environments and Technology

4.1. General Use

Learners must:

- Use QA resources for legitimate purposes only
- Follow instructions provided by QA staff
- Maintain professional conduct at all times

4.2. Prohibited Activities

Learners must not:

- Access or attempt to access unauthorised systems or data
- Disrupt training sessions, platforms, or users
- Introduce malicious software or tools
- Conduct unauthorised technical activities outside approved exercises

4.3. Acceptable Use of Assets

All QA assets must:

- Be used securely and appropriately
- Not be copied, modified, or removed without permission
- Be protected against unauthorised access.



4.4. Intellectual Property

All training materials remain the property of QA and/or third parties.

Learners must not:

- Copy, reproduce, or distribute materials
- Upload materials to external platforms or AI tools
- Use materials beyond personal study
- Create derivative works or deliver training using QA content

This applies whether content is accessed during live sessions, recordings (where permitted), or provided materials.

4.5. Recording of Training Sessions

General Rule

Recording is **strictly prohibited** unless explicitly approved, including recordings kept for personal use.

This includes:

- Audio and video recording
- Screen capture
- Secondary or undisclosed devices

Virtual Sessions and Vendor Content

Learners must not:

- Record virtual sessions using personal tools or devices
- Use screen recording software, browser extensions, or meeting assistants
- Capture content delivered by third-party vendors

Where vendor/ third party materials are used:

- Content remains protected intellectual property
- Recording or redistribution is prohibited unless authorised
- Vendor/ third party-specific restrictions must be complied with



Approved Recordings

Where recording is authorised:

- All participants must be informed
- QA-approved platforms must be used

Recordings:

- Are for personal study use only
- Must not be shared, copied, or distributed
- Must not be uploaded to external platforms or AI tools
- May be subject to time limits

Circumvention

Learners must not:

- Circumvent technical controls
- Use hidden or background recording tools

4.6. Use of Artificial Intelligence (AI)

Restrictions

Unless explicitly authorised, learners must not use AI tools to:

- Record, transcribe, or summarise sessions
- Capture training content
- Upload course materials into external systems
- Generate outputs based on confidential or proprietary information

Tools in Scope

This includes, but not limited to:

- Generative AI tools and chatbots
- Automated note-taking or transcription tools
- Meeting assistants and transcription services
- Browser extensions and integrated platform tools

Permitted Use

AI may only be used where explicitly authorised or approved as a reasonable adjustment.

Relevant participants must be informed where applicable.



Data Protection Considerations

AI tools may:

- Breach confidentiality
- Violate legal and contractual obligations

4.7. Use of External Platforms

Learners must:

- Comply with terms of third-party platforms used in training
- Not upload QA content to external systems, including AI tools

QA is not responsible for:

- Third-party platform outages
- External data handling practices

5. Confidentiality and Professional Conduct

5.1. Confidentiality

Learners must:

- Not disclose confidential information relating to QA, other learners, employers, clients, or training content
- Treat group discussions and breakout sessions as confidential
- Avoid sharing employer's sensitive organisational information unless authorised and appropriate

When sharing screens, learners must ensure:

- No personal or confidential data is visible

5.2. Professional Conduct

In all environments, learners must:

- Communicate respectfully
- Use appropriate language and behaviour



- Avoid disruptive conduct

For virtual sessions:

- Manage microphones appropriately
- Use chat functions professionally
- Minimise distractions

5.3. Use of Corporate Devices

Learners are responsible for complying with their organisation's policies when using corporate devices or networks.

QA is not responsible for:

- Restrictions imposed by employer systems
- Connectivity or access issues relating to such environments

6. Online Safety and Behaviour

Learners must:

- Act respectfully and inclusively
- Avoid harassment, discrimination, or inappropriate behaviour
- Maintain a safe and supportive learning environment

Inappropriate behaviour may result in removal from training sessions.

7. Compliance and Enforcement

7.1. Reporting

Learners must promptly report:

- Policy breaches
- Security incidents
- Suspected unauthorised recording
- Data protection concerns



Learners should report incidents as soon as possible via:

- Their QA instructor; or
- QA support channels, as communicated at the start of the training - [Live Chat](#)

Reports should include sufficient detail to enable investigation, such as the date, session and nature of the concern.

7.2. Non-Compliance

Examples of non-compliance include:

- Unauthorised recording
- Misuse of AI tools
- Breach of confidentiality or intellectual property

7.3. Enforcement

Any breach of this Code of Conduct will be taken seriously and may result in action taken by QA. Such action may include:

- Issuing warnings
- Removing learners from sessions
- Restricting or revoking access to systems
- Notifying relevant stakeholders
- Taking further action where required by law, contract or QA policy

7.4. Liability

Learners may be personally liable where actions:

- Breach applicable laws
- Cause loss, damage, or unauthorised disclosure

8. Review and Maintenance

This Code will be reviewed annually or following significant changes.

Next review: June 2027



Schedule A: Recording Guidelines

A1. Conditions

Recording may only occur where:

- Approved in advance
- Clearly communicated
- Where required, appropriate consent or another lawful basis is confirmed

A2. Usage Restrictions

Authorised recordings:

- Are for personal study only
- Must not be shared, copied or redistributed
- Must not be uploaded to AI or external platforms
- Must be securely stored
- Must be deleted when no longer required

A3. Additional Controls

- Secondary or hidden recording devices are prohibited
- AI transcription or note-taking is treated as recording
- Vendor content may not be recorded where restricted

A4. Enforcement

QA reserves the right to:

- Stop recordings immediately
- Remove participants
- Take appropriate action in response to breaches