QA IN LEARNING CODE OF CONDUCT

Date of Issue: March 2024

PUBLIC

This document may be disclosed outside of the QA group of Companies.

Version Control

Revision History			
Version	**Issue Date**	**Author**	**Description of Change**
1.8	21/03/2024	G Sayer	Updated with learner content from QA Computer User Agreement. Layout revised.
1.7	05/10/2023	Stephen Smith	Document name change from QA Learner Code of Conduct to QA In Learning Code of Conduct. Minor font changes.
1.6	15/05/2023	DJ Black Stephen Smith	Added content around Safeguarding.
1.51	23/03/2023	DJ Black	General review and update to paper handling, process for recording of in class proceedings and other minor updates.
1.50	04/04/2022	Simon Kent	General review and update
1.42	16/02/2021	DJ Black Tracy Johnson	Senior Service Delivery Manager
1.41	14/01/2020	Glen Marshall DJ Black	Review and updated template.
1.4	06/09/2018	DJ Black	General review and update
1.3	23/03/2017	DJ Black	Updated to include recording of classroom sessions and development of malicious code.

Document Approval		
Name	**Position**	**Viewed / Comments**
Mike Brown	Director of Technology and Security Services / CISO	Approved
Simon Kent	Head of Operations	Approved
Stephen Smith	Safeguarding Manager	Approved

CONTENTS

1 Introduction

1.1 Overview

This Code of Conduct applies to all learners studying with the QA group of companies (hereafter “QA” or “Company” or specifically “QAHE”), including apprentices and other delegates in addition to the Instructor community. Instructors are also bound by the QA Computer User Agreement as employees or representatives of Company.

This Code of Conduct provides policy surrounding activities that you may undertake while within Company training centres or within other Company classroom or learning environments, including those online or indeed the wider community as a whole.

Cyber Defence and Offence, amongst other teachings, are sensitive subjects, and you shall not bring Company, your sponsor or employer into disrepute as a result of your misplaced actions.

1.2 QA Higher Education Students

Students of QA Higher Education (QAHE) should read applicable QA/QAHE policy documents along with the relevant parent University policy documents.

Within this QA Code of Conduct use of the word 'delegate' includes student users within a QAHE site or campus.

1.3 Definitions

A Classroom is defined as the space within which education or presentations are delivered. This may be a room or indeed an open area depending on the event.

Event Delivery Infrastructure is defined as the computer and network infrastructure at the boundary of and outside of the classroom environment that you are within.

Classroom Infrastructure is defined as the equipment logically within your classroom, which your Instructor has given you permission to use or access.

Typically the limit of the Classroom Infrastructure environment will be the wired or wireless LAN default gateway leading from the in-classroom network you are on and leading to the Internet and other networks.

Personal data includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- can be indirectly identified from that information in combination with other public information.

2 Legal Notice

You must not perform or participate in any form of illegal activity (or any activity that would be generally considered unacceptable or indecent) using the equipment, services or skills provided to you by Company or your employer.

You must always ensure that you are aware of the laws that are applicable to the tasks that you undertake, including those of other territories (countries) based on the locations of the systems you are accessing.

You are solely responsible and liable for any direct, indirect or consequential loss or damage arising from your actions or in connection with our service, whether arising in tort, contract, or otherwise – including, without limitation, to Company or any third party, any loss of profit, contracts, business, goodwill, reputation, data, income or revenue.

You must always ensure:

- You have permission to undertake the task from the system or asset owner or their verified representative.
- You assess the risk - consider the ownership and impact of all systems that could potentially be affected by the task – these may be outside of the originating country.
- You are aware of the applicable laws and if in doubt seek legal counsel in advance.

You are wholly responsible for **your** actions.

Ensure that you understand the above and agree to be bound to the conditions presented within this document.

3 Monitoring

Company (and in some cases, your employer), reserve the right to monitor and audit all training centre network and device activities, which could include your user credentials on sites you may visit such as social media, webmail and/or personal banking.

Data may be captured within the auditing tasks, which could inadvertently include personal data – and potentially could include your passwords. If the user wishes to avoid the possibility of their personal data being captured, they should not use any Company or training systems to access such services.

The monitoring and auditing tasks are undertaken on a continual basis to ensure compliance with this along with other Company policies and statutory requirements.

4 Training Infrastructure and Environment

4.1 General

Your use of equipment and services are provided to support your learning while you are with us, and unless otherwise communicated in writing to you, remain the property of Company or your employer.

4.2 Prohibited Activities

Event Delivery Infrastructure must not be abused, attacked or probed in any form, including but not limited to:

- Personal data must never be used in any uncontrolled environment or system, such as within a classroom, training, test, lab or development environment.
- Removal or otherwise making any network or security control that Company or their partners have deployed ineffective.
- Scanning of ports.
- Sniffing of wired or wireless network traffic unless directed by the Instructor within the boundaries a classroom.
- Attempts to circumvent or disable any means of identity management or authentication.
- Use of any man in the middle exploits.
- The Company Delegate Wireless service (TRAINING_AP_PUBLIC) or other non-classroom shared service must not be used for any learning or development activities.
- Use of exploits against any Company or network owner device without direct permission from an Instructor.
- Attempts to disable or gain access to any physical access control system, swipe cards or other mechanism.
- Session hijacking – no attempts to impersonate through use or abuse of another token, cookie, user or entity.
- SQL injections – any exploit to craft SQL responses or run scripts.
- Brute Force.
- DoS/DDoS attacks.
- DNS poisoning.

4.3 Unacceptable Use

Use of Company's computing facilities are subject to the user's acceptance of this policy. Misuse of these facilities will be considered a breach of Company Policy and may result in removal from your course of study, disciplinary action or dismissal by your employer or prosecution.

Company systems must not be used to download, disseminate, send, receive, store, distribute, transmit, post, stream, upload or display material that is or could be considered to contain material that is illegal or inappropriate. You must also ensure that you do not breech any copy write attached to the materials accessed or downloaded.

Any action in doing so will lead to disciplinary or legal action being taken by Company or your employer and may also constitute a criminal offence.

Inappropriate material includes, but is not limited to:

- Child abuse
- Bestiality
- Rape
- Pornography
- Sexism
- Violence
- Racism
- Defamation
- Torture
- Extremist ideology
- Other illegal, immoral or indecent material

Should a user receive any suspect material, outside of that provided by your Instructor, or become aware of any location of such material, the incident must be reported immediately to the Company IT Service Desk (ITServiceDesk@qa.com or by phone UK +44 (0)113 382 6200 or USA toll free +1(800) 300-2652).

Users are personally responsible for exercising good judgment regarding the reasonableness and extent of personal use of Company facilities. Users should be guided by the policies detailed within this document to ensure their use is appropriate, and if there is any uncertainty or doubt, users must consult their manager, Instructor or the Company IT Service Desk to gain clarification.

Company IT services must not be used for personal financial gain.

You must never send an email purporting to be from any Company domain unless the email account or domain has been directly issued to you for your own personal or in class use.

Any misuse of Company or other third party computing systems involving criminal activities may result in summary dismissal and/or the user being reported to the relevant authorities.

Company utilise comprehensive toolsets to monitor, control and document the use of network controlled PCs and devices. Where any delegate or student is found to have breached any policy rule within this document, the incident will be reported to their employer and, where appropriate, relevant authorities.

Bullying of any nature will not be tolerated, this can include but is not limited to: harassment, denigration, flaming, cyber stalking or exclusion.

4.4 Cyber Training Course Obligations

Company provides a range of courses relating to cybersecurity, including penetration and vulnerability testing.

Company are not liable for your misuse, intended or accidental, of any penetration or malicious techniques you have learned within your time with Company.

Ensure you are familiar with the requirements of the UK Computer Misuse Act 1990, the Serious Crime Act 2015, the Communications Act 2003, the Telecommunications Act 2000, and all published amendments. Other legislation may also be applicable, particularly if studying from other regions.

Where cyber type learning is being undertaken, and should your target or network over which the target is reached be outside of the UK, you must acquaint yourself with the target country and state laws and policies relating to the task you are to undertake as they vary considerably and often more comprehensively within non-UK territories.

Any cyber security or hacking skills you may have are only to be practiced while within the safe boundary of a classroom or other safe environment.

You must always obtain full written and explicit permission from the target system owner before performing any exploit or penetration activity. To be clear – if you do not have permission of the system or asset owner, you must not perform activities of any sort against the device or entity.

4.5 Acceptable Use of Assets

Company may issue you with a device or other asset for your use while with Company. The points below provide guidance as to the acceptable use of the device:

- The device or asset will not be used to store any host organisation (sponsor or employer) related, personal, or above “OFFICIAL” or “PUBLIC” information.
- You are responsible for the safe and secure storage and handling of the asset(s).
- The asset(s) will be locked away in your personal locker or other agreed secure storage when not in use.
- The asset(s) issued to you will not be removed from the training centre in which they were issued unless under direct instruction and written permission from a Company Instructor.
- Company and the relevant sponsor or employer retain the right to audit the contents of any storage devices and their storage location.
- You are responsible for the backup of any data that is contained within the asset(s).
- The asset(s) remains the property of Company and are to be returned on request.
- Assets that have not been personally assigned to you must not be removed from the classroom in which they were provided without written Instructor permission.
- Assets that have not been personally assigned to you must not be removed from the Company centre in which they were provided without written permission from the Company IT Service Desk.

4.6 Delegate and Student use of Class and Campus IT Facilities

The Company provides internet access free of charge within the University campus and training centres. This is provided by means of kiosk PCs in the coffee areas and where the course setup permits, on PCs within technical classrooms.

Many of Company's centres have free delegate and student wireless internet access. Delegates and students will find the wireless access details (SSID and passcode) on noticeboards within the centres.

Internet service is provided as-is, with no promise of any service level, security or availability guarantee.

Use of the internet access is subject to a fair use policy. Delegates and students should not abuse the service, such as instigate downloads of data that may impact the overall available bandwidth. Where abuse is detected, Company may remove the internet service without notice.

All delegates and students must abide by Company's policies on prohibited and unacceptable use, as detailed in this document.

Although not encouraged, delegates are permitted to connect USB devices to classroom devices. This includes USB devices and mobile phones. Delegates should however be reminded that Company delivered courses are comprised of copyright materials, with the IPR retained by Company and therefore should not be copied.

Should a delegate or student connect their own devices to a Company device, they are doing so at their own risk. The Company shall not be held liable for any damage or data loss as a consequence of the action.

Users are reminded that any cyber security or hacking skills that may be learned while they are with Company are only to be practiced while within the safe boundary of a classroom. Refer to the conditions described in section 4.4 above.

4.7 Recording of Video or Audio

Recording of video or audio may be desirable within Company's centres to aid learning.

Any delegate or student requests to perform audio or video recording must be made at the time of event booking.

Where justification is accepted, all delegates or students must be made aware prior to the start of the recording, so that they are aware and agree to participate in the event. Should any one delegate or student oppose the recording on the day, then no recording will be made.

Where Company will be streaming or recording the event, notice of this will be communicated within the joining instructions that are sent once the booking has been confirmed.

4.8 Public Internet Usage

The use of Internet access provided within Company premises is provided free-of-charge, and you acknowledge and accept that it is unreasonable to hold Company liable in respect of the use of this service and the information accessed via this service.

The internet access is provided for the purposes of general browsing and research only. Please do not abuse the facility.

If anyone is found to be downloading large files from the internet, and it causes a bandwidth issue within the centre, internet access may be removed as a provision to the classroom. Internet access is monitored.

Company is not responsible for the content at any of the external sites accessed via Company networks or computer equipment. Furthermore, although computer equipment is maintained, its confidentiality and integrity cannot be guaranteed against the presence of viruses or any other types of malware.

Internet service is provided as-is, with no promise of any service level, security, integrity or availability guarantee.

4.9 Intellectual Property and Copyright

Intellectual Property (IP) is the term applied to a type of property or asset arising from the output of a human mind - essentially the material representation of an idea.

Intellectual Property Rights (IPR) are the legal rights given to the creator to protect the invention or creation, allowing them to achieve some commercial benefit from their efforts and recover research and development costs. This is commonly achieved through protections like copyright, patents and trademarks.

Copyright laws aim to prevent others from copying, distributing or adapting the IP. Copyright applies to, amongst other things, any written work, including software and databases, and artistic work, including diagrams. The Company's products including its coursework and course materials are key parts of its IP and, whilst protected by copyright laws, should be handled and shared with care and consideration.

Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, logos or trademarks, books or other copyrighted sources, copyrighted music, video and the installation of any copyrighted software for which Company or the end user does not have an active license is strictly prohibited.

All users, including delegates, apprentices and students are reminded that Company delivered courses and events are comprised of copyright materials and therefore should not be copied or distributed by any means without written permission of Company.

4.10 Handling of Paper

Generally all paper within classrooms is to be limited to Company's PUBLIC classification. This means that no CONFIDENTIAL, INTERNAL or UK Government 'OFFICIAL' marked materials are to be processed.

Where events require any material classified above PUBLIC or OFFICIAL, the Instructor or Tutor is responsible for the security of the item.

The waste bins within the training areas are handled as recycling material or general waste and are not securely disposed of. Where classroom papers require secure destruction, the Instructor or Tutor must use the Company confidential waste bins or on-site cross-cut shredders.

5 Online Safety

Learners undertaking apprenticeships at all levels and in line with auditor expectations will be informed about online safety, as part of information sharing during 1-2-1 reviews or as part of engagement with Company's Safeguarding teams.

You will receive information to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting your online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns.

You will be expected to know:

- Your rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- What material not to provide to others that you would not want to be shared further. Additionally, knowing not to share personal material, which is sent to you.
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how you behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if you have been affected by these behaviours
- It is not permitted to record or photograph staff or learners without the tutor and the subject's express permission

The Counter-Terrorism and Security Act 2015 places a duty on everyone to have "due regard to the need to prevent people from being drawn into radicalisation or terrorism". All users are expected to be vigilant in spotting any use of IT or Company resources to further extremist ideology or share extremist messages or goals. Company systems and software must not be used to access any extremist material or publish / share extremist views or opinions which are contrary to British values or promote illegal activity. Users must remember that Company systems are monitored, and should any instances be identified, Company will report the incident to the relevant agency.

6 Compliance

6.1 Policy Compliance

Company Management expects that all learners will comply with this Code of Conduct.

6.2 Penalties

Non-compliance is defined as any one or more of the following and may result in penalties:

- Any person who knows of or suspects a breach of this policy must report the facts immediately to their Company contact, e.g. Instructor, Tutor or Skills Coach or, where that person may be involved in the breach, to their booking contact or other formal complaint contact.
- Any violation or non-compliance with this policy may be treated as serious misconduct, which may lead to termination of employment, and/or civil or criminal prosecution.

6.3 Liability

Clearly, any breach can result in liabilities surrounding the incident. Depending on the nature of the incident, the individual may be personally liable in addition to or instead of Company, particularly in instances breaching legislation. Therefore, a learner that breached legislation may be held accountable and prosecuted as an individual, and may be personally responsible for any fines that are imposed on them by the authorities.

7 Code Review and Maintenance

This Code of Conduct shall be reviewed by a member of the Information Security Forum annually or whenever there is a significant change that may affect its content, e.g. legislation, strategy or organisation. Changes shall be approved by the Chief Information Security Officer (CISO) or delegated approver.