QA IN LEARNING CODE OF CONDUCT

Prepared by: David J. Black

Prepared for: Mike Brown

Date: October 2023

Issue: V1.7

PUBLIC

Distribution of this document is not controlled therefore can be shared with anyone.

Version Control

Document Information	
1.7	Document name change

Revision History			
Version	**Issue Date**	**Author**	**Description of Change**
1.7	05/10/2023	Stephen Smith	Document name change from QA Learner Code of Conduct to QA Online Safety Policy and In Learning Code of Conduct. Minor font changes
1.6	15/05/2023	DJ Black Stephen Smith	Policy consolidation with Online Safety Policy.
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. Review and updated template to incorporate online learning and safety.
1.42	16/02/21	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.
1.2	04/04/16	DJ Black	Updated to broaden application and use.
1.1	18/08/15	DJ Black	Updated wording around monitoring to aid clarity.
1.0	24/07/15	DJ Black	Initial release.

CONTENTS

1 Introduction

The purpose of this document is to provide guidance and communication of policy surrounding activities that you may undertake while within QA centres or within other classroom 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 QA, your sponsor or employer into disrepute as a result of your misplaced actions.

This policy applies to all learners, including apprentices and other delegates in addition to the Instructor community.

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 QA 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 QA 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.
- 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.
- Be aware of the applicable laws and if in doubt seek legal counsel in advance.

You are wholly responsible for your actions.

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

3 Monitoring

QA (and in some cases, your employer), reserves 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 QA 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

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 QA or your employer.

4.1 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.

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 QA 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 such as wardriving.
- Use of any man in the middle exploits.
- The QA 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 QA 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.

5. Online Safety

While new technologies are enhancing communication and creativity some are also challenging the definitions and boundaries of the adult education environment. As active participants in a digital world, our broad curriculum and our learners' personal goals requires regular use of a variety of IT systems and communication tools. Our aim is to provide learners and staff with the knowledge, skills and confidence to become safe and responsible users of technology.

This policy relates the QA's learners who have access to and are users of IT systems and resources, and applies to all electronic devices and services provided, including the use of computers, mobile phones and related equipment, regardless of ownership, where they are used on premises for which QA has responsibility or use an internet or other network connection for which QA has responsibility.

For security reasons, use of the internet and e-mail services provided by QA may be recorded by QA. This may include details of sites visited and addresses of emails sent. However, QA will not monitor details entered into secure web pages, or the content of e-mails where provided by another Internet Service Provider.

Privacy and confidentiality: Because equipment may be used by several different people, QA cannot guarantee the privacy of personal data, including e-mails. It is the responsibility of users to ensure they correctly log out of any websites, e-mail packages or other programmes before leaving the computer/device.

QA learners and staff may use QA equipment for legitimate activities related to a learning programme run by or for QA. These activities must be within the law and must not be prohibited elsewhere in this policy.

6. Online Safety Aims

QA aims to:

- Have robust processes in place to ensure the online safety of learners, staff, volunteers and Board Members
- Deliver an effective approach to online safety, which empowers us to protect and educate the QA learning community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Ensure learners, staff, volunteers and Board Members are responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use

7. Legislation and Guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools, colleges and training providers.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on learners' electronic devices where they believe there is a 'good reason' to do so. However, where the image relates to a minor the police should be called to take possession of the device in question.

Prevent Duty - There is a duty on authorities under the *Counter Terrorism and Security Act 2015* to have due regard to the need to prevent people from being drawn into terrorism. As with other online harms, every tutor needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

QA has a vital role to play in protecting its learners from the risks of extremism and radicalisation. Keeping learners safe from risks posed by terrorist exploitation of social media will be approached in the same way as safeguarding learners from any other abuse.

If you have a concern for the safety of a learner at risk of radicalisation, you should follow the steps in QA's Safeguarding Policy & procedures, including discussing your concerns with QA's designated safeguarding lead (DSL).

8. Roles and Responsibilities

8.1 The Safeguarding Governance Board

The Board has overall responsibility for monitoring this policy and holding the

Designated Safeguarding Lead (DSL) to account for its implementation. The board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the DSL.

All Board Members will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the QA's IT systems and the internet. This can be found in the Computer User Agreement Policy, within the governance section.

8.2 The Designated Safeguarding Lead

Details of QA's DSL and deputy are set out in our safeguarding policy and Procedure. The DSL takes lead responsibility for online safety at QA, in particular:

- Ensure that staff understand this policy and that it is being implemented consistently throughout the organisation
- Working with the IT team and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy and the Safeguarding Policy and Procedure
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the QA's Learner-Provider Code of Conduct
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

8.3 IT Service desk

The IT team works with the DSL and are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners safe from potentially harmful and inappropriate content and contact online while at QA, including terrorist and extremist material
- Ensuring that QA's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring QA's IT systems on an agreed basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring any online safety incidents are logged in line with IT procedures

- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with QA's learner Bullying policy

This list is not intended to be exhaustive.

8.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the QA's IT systems and the internet, and ensuring that learners follow the QA's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with QA's Safeguarding Policy and Procedures

This list is not intended to be exhaustive.

8.5 Learners

Learners are expected to:

- Notify a member of QA staff with any concerns or queries regarding this policy
- Ensure they have read, understood and agreed to the terms on acceptable use of QA's IT systems and internet which can be provided by your regular QA contact.

9. Educating Learners About Online Safety

Learners will be taught about online safety as part of continued updates and information sharing, in line with QA Safeguarding obligations.

Learners will be taught to:

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

Learners should know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online/social media/WhatsApp
- 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
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- 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 they 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 via all online mediums (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- It is not permitted to record or photograph staff or learners without the tutor and the subject's express permission

The safe use of social media/WhatsApp and the internet will be covered where relevant.

QA will use a range of platforms to raise learners' awareness of the dangers that can be encountered online.

10. Cyber-Bullying

10.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also QA's Learner Bullying policy and Safeguarding Policy and Procedure.). Available via your regular QA contact.

10.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that learners understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

QA will actively discuss cyber-bullying with learners, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Tutors are encouraged to find opportunities to use aspects of their course to cover cyber-bullying.

All staff, Board Members and volunteers (where appropriate) receive updates on cyber-bullying, its impact and ways to support learners, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, QA will follow the processes set out in the QA Safeguarding Policy & Procedure.

Where illegal, inappropriate or harmful material has been spread among learners, QA will use all reasonable endeavours to ensure the incident is contained. It is not permitted to record or photograph staff or learners without the tutor and the subject's express permission.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

11. Acceptable Use of the Internet at QA

All learners are expected to agree to the acceptable use of the QA's IT systems, details can be found in the Computer User agreement Policy or QA Learner Code of Conduct (Appendix 1). Visitors will be expected to read and agree to QA's terms on acceptable use if relevant.

Use of QA's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

QA will monitor the websites visited by learners, staff, volunteers, Board Members and visitors (where relevant) to ensure they comply with the above.

More information is set out on acceptable use within the Code of conduct & QA Computer User Agreement.

12. Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety. Any

Incidents or reports can be provided.

This policy will be reviewed every year by the Safeguarding Manager and QA's IT department.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding Policy and Procedure
- QAA Learner Bullying policy
- Staff disciplinary procedures
- QA User Computer user agreement
- QA Learner-Provider Code of Conduct
- IT and internet acceptable use policy

14 Public Internet Usage

The use of Internet access provided within QA group premises is provided free-of-charge, and you acknowledge and accept that it is unreasonable to hold QA 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.

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. Please do not abuse the facility.

QA is not responsible for the content at any of the external sites accessed via QA 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.

15 Unacceptable Use

Use of QA'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.

QA 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 QA or your employer and may also constitute a criminal offence.

Inappropriate material includes, but is not limited to:

- Child abuse
- Pornography
- Racism
- Defamation
- Torture
- Other Illegal, immoral or indecent material
- Bestiality
- Sexism
- Violence
- Rape
- Extremism
- Bullying

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 QA IT Service Desk ITServiceDesk@qa.com (phone 0113 382 6200).

Users are personally responsible for exercising good judgment regarding the reasonableness and extent of personal use of QA 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 QA IT Service Desk to gain clarification.

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

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

Any misuse of QA or other third party computing systems involving criminal

activities may result in summary dismissal and/or the user being reported to the relevant authorities.

QA utilise comprehensive toolsets to monitor, control and document the use of network controlled PC's 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.

You are reminded that QA are not liable for misuse of any penetration or malicious techniques you may have learned within your time with QA. Please ensure you are familiar with the requirements of the UK Computer Misuse Act 1990 including 2008 revisions, the

Serious Crime Act 2015, the Telecommunications Act 1984 and other applicable legislation.

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.

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

16 Acceptable use of Assets

QA may issue you with a device or other asset for your use while with QA.

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 QA Instructor.
- QA 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 QA Group 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 QA centre in which they were provided without written permission from the QA IT Service Desk.

17 Recording of Audio or Video

Recording of audio or video may be desirable within QA'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 QA 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.

18 Paper Handling

Generally all paper within classrooms is to be limited to QA's PUBLIC classification. This means that no CONFIDENTIAL, INTERNAL or Government marked 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 paper bins within the training areas are handled as recycling material and may not be securely disposed of. Where classroom papers require secure destruction, the instructor or Tutor must use the QA office provided shredders or secure bins.