APA
& Procurement Supply Training

Digital Safeguarding Policy and Procedures

CIPS
Centre of Excellence

APA Digital Safeguarding Policy

APA Procurement Training Ltd undertakes a range of activity in the digital space that includes group and individual tuition, meetings, communication, data gathering and storage and information sharing. As a training provider, one of our primary activities is using digital technologies to connect with learners from across the United Kingdom and beyond and working with them to develop the knowledge, skills and behaviours they need to succeed in procurement, supply chain and related professions.

APA recognises that there are a range of different safeguarding risks associated with digital engagement with learners, employers, partner organisations and other stakeholders, as there are with physical engagement with these parties. This Digital Safeguarding Policy has been developed in order to address these risks and this ensure that we are keeping our learners and all others we work with safe from harm. This Digital Policy should be read in conjunction with APA's Safeguarding Policy.

Commitment to Digital Safeguarding

Everyone, without exception, has the right to protection from abuse and exploitation, regardless of factors such as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief or sex or sexual orientation. Safeguarding individuals and their organisations from such harm while they learn or interact with us in the digital space is a key organisation responsibility and the focus of this policy.

At APA, we are committed to:

- Establishing and operating policies and procedures on using digital platforms that enable our learners, client organisations, employees and partners to stay safe in their online interactions with us.
- Providing our learners with information, advice and skills on using digital platforms and staying safe online
- Taking appropriate steps to safeguard our learners online, and especially those adults deemed 'at risk'.
- Developing and reviewing our policy and protocols regularly.

Digital Risk

APA Procurement Training Ltd seeks at all times to minimise the risk of a Digital Safeguarding incident occurring as a result of its engagement with learners, employees, client organisations and partners.

There are a number of key forms of Digital Risk:

- Conduct – these risks are focused on of the activities of the user of APA digital platforms and the extent to which they may engage in inappropriate behaviour towards others or towards a wider audience – such as by bullying, harassment, or posting offensive material.
- Content – these risks concern exposure to inappropriate content and unreliable information while using APA digital platforms.
- Contact – these risks occur through direct contact with other users in the APA digital space and include such activities as bullying, trolling and online grooming.
- Commercial – these risks include the financial and personal consequences of online fraud or theft such as for example through 'phishing' or other methods of identity theft.

APA maintains an up to date understanding of the current cyber threats and different digital risks that impact may impact organisations. One of the ways in which this is achieved is through core membership of the Cyber Resilience Centre for the South West. This is a police-private partnership that shares information, advice and provides a range of business services to increase online safety and make organisations more cyber resilient.

Examples of safeguarding incidents might include:

- Bullying/trolling
- Threats of harm
- Posting personal information that can identify and locate an 'at risk' person
- Sexual grooming, luring, exploitation and abuse contact with strangers
- Harassment or impersonation
- Exposure to inappropriate content, including indecent images / sexual content, profanity, spam, advertising, URLs that lead to material not authorised/endorsed by FLN etc;
- Involvement in making or distributing illegal or inappropriate content
- Theft of personal information
- Exposure to information and interaction with others who encourage self-harm/suicide
- Exposure to racist or hate material
- Encouragement of violent behaviour and the recording of an assault for the purpose of widely sharing the recording
- Promoting violence and acts of terrorism
- Glorifying illegal activities such as drug taking
- Defamation and/or breach of copyright.

A Digital Safeguarding Incident can occur anywhere across APA's digital space. This space is broad, because it comprises everything the organisation does online which includes our own platforms such as our website, our online teaching software and our learner, knowledge and resource databases and information sharing services. It also includes our social media channels including Facebook, Twitter and LinkedIn.

In addition to the 'official' digital output of our organisation – that is, content created at the direction, or with the endorsement of the APA - there is potential for significant 'unofficial' digital output. This 'unofficial' footprint includes APA employee, learner, and partner generated content (such as reviews or posts in networking groups) and more unofficial content generated without any input or consultation with APA. We recognise that this 'unofficial' content can also pose significant digital safeguarding risks, particularly in relation to social media channels.

Digital Monitoring

APA Procurement Training Ltd actively monitors our digital space and those social media platforms where both official and unofficial content might exist. Two types of monitoring is undertaken in relation to APA digital activities:

Content – all APA digital content across all of the platforms on which it is published is monitored by our designated Digital Monitor, Nicky Hingston, on a daily basis. The Digital Monitor works closely with the Designated Safeguarding Lead wherever any Safeguarding concerns arise. The Digital Monitor has the authority to remove ANY content of any nature that is deemed inappropriate, report the creator and the content to the relevant digital / social media channel, and escalate to relevant authorities (including law enforcement authorities), if appropriate. The Digital Monitor will act without waiting for a second opinion from anyone, if they feel the situation merits such action. APA's policy in this regard is to act first to remove inappropriate content as a priority,

Process – the operation of IT and digital systems over which APA has control is monitored by our designated Systems Administrator, Personic Computers, through remote monitoring software. This includes continuous system performance monitoring, proactive threat management through dedicated anti-virus software, email threat protection, patch management and active health check. Threats and performance issues are identified in real time and reported by the Systems Administrator to the Designated Safeguarding Lead to assess the threat that they may pose. Initial discussions will determine appropriate action, including informing any stakeholders impacted and agreeing remedial action. Outside of current threats identified a monthly reporting and review process is used as a basis for ongoing improvement.

Account Security

APA Procurement Training Ltd is committed to maintaining account security across all of the digital services we use to communicate and interact with learners, clients, employees and partners.

A cornerstone of account security is effective password protection. We have developed a strong password policy that is communicated to all employees and will be applied for learners when they are given access to our information sharing service – see APA Password Policy.

Our key online training delivery service is Zoom. All tutors are provided with training on this application to ensure that security is maintained. Zoom software updates are applied to all machines through which online training is delivered when they are issued. Session invites are sent out only to learners identified secure email addresses and are not publicly shared or published anywhere where they may be seen by other parties. A waiting room system is used to ensure that those being admitted to sessions are only those invited.
Our email service is provided by Microsoft. Administrator access to this service, which is required to change our domain or to add new users, is available only to the Directors. The email addresses we use to communicate with learners, clients, internally and with partners, either directly or through our social media accounts, will always use the "apatraining.co.uk" domain. Passwords for these accounts are held centrally by Directors and by the Digital Monitor. The changing of usernames/handles, email addresses and passwords for these accounts is prohibited without the authorisation from Directors.

Any new information sharing platform, training delivery service or social media account will only be created with the approval of the Directors. This is to ensure that every account is consistent with the guidelines set out in this policy.

APA takes all breaches of security seriously, and will act to improve account security at every opportunity and will consider all disciplinary options available to it in response to a security breach. This includes anything from suspension of access, additional training, consultation, through to termination of relationship in the most persistent and serious of incidences.

Data Protection

APA's Privacy Policy outlines how we protect the privacy of others and adhere to data protection laws in relation to any personally identifiable information that is collected, stored, used, or shared. We recognise that additional measures may, from time to time, need to be taken with regard to data protection in a Safeguarding context.

In situations where leaners deemed at risk may need extra protection, APA will seek to protect identities and moderate content accordingly, with only agreed identifiers and non-identifiable locations used. Agreed identifiers maty include changed names or pseudonyms, which may be footnoted with the following: "Names have been changed in order to protect the identities of those involved".

Informed Consent

APA will only publish information and images, still or moving, where we have received informed written consent, from the learner, client or partners featured. We will ensure individuals can see how content featuring them is being used and shared, disclose any potential risks, and ensure individuals are aware of their rights so that informed consent can be given. Third parties supplying content to APA will be required to demonstrate that they have acquired written consent from those featured.

Trusted Content

APA endeavours to share information that is factually accurate, up to date and follows the latest best practice. Due diligence is carried out to ensure that content shared is truthful and adheres to these principles. Content will not click through to unexpected destinations and will only link out to trusted and relevant third parties.

Policy review

This policy is reviewed annually.

Approved by the Senior Management Team APA.

Last reviewed March 2025.