



Summary of Main Changes to the Specialist Quality Mark from 1 October 2022

Background

1. The Legal Aid Agency (LAA) has reviewed and updated the Specialist Quality Mark (SQM) Standard and SQM Guidance. A summary of the main changes are set out in the table below. The revised requirements in the SQM will come into force on 1 October 2022. They will apply to all applications for a Desktop Audits and all requests for a Pre-Quality Mark Audit or a Post-Quality Mark Audit after this date.

Summary of main changes to the SQM

Requirement	Change
A1.1 Your business plan	A new requirement has been added to make sure organisations have internal procedures in place to ensure clear lines of communication. This must as a minimum include the following: <ul style="list-style-type: none">• An internal communications plan• A regular cycle of team meetings.
A4.1 Safeguarding policy	A new requirement has been added requiring organisations to have a written safeguarding policy is in place setting out the procedures that are in place to keep children, young people and vulnerable adults safe and respond to any safeguarding concerns.
C1.4 Modern Slavery Legislation	A new requirement has been added to ensure that organisation take steps to identify whether there is any action they need to take to comply with modern slavery legislation.
C2.1 Financial responsibilities	A new requirement has been added to ensure that organisations covered by Part 3 of the Criminal Finances Act 2017 have procedures in place to prevent enabling of criminal tax evasion by associated persons.
C2.5 Anti-Money Laundering Policy	A new requirement has been added to ensure that organisations that are required to comply with the <i>Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017</i> have an appropriate Anti-Money Laundering Policy in place.
F6.1 Information handling	A new requirement has been added to ensure that organisations have in place procedures to ensure client data is kept secure at all times and to protect the personal data from unauthorised or unlawful processing, accidental loss, destruction or damage and to maintain the confidentiality, integrity and availability of information