End User - Security and Compliance

Phishing

Users should be aware of common phishing attacks. Any automated emails generated and sent by the system are limited and only include invitations to create an account and password reset codes. The system will never ask for any credentials via email or send links to be followed.

Malware protection

It is very important that the security on users' devices is kept fully up to date and so they should have all the latest updates for their operating system and malware protection should be installed where required (e.g on Windows)

Network security

Users should also be aware of network security issues. Using unsecured public WIFI has its risks. However, considerable care and due diligence has gone into the security of Quantum and the system is fully encrypted making these risks minimal.

Multi Factor Authentication is the best protection against login theft and its use is strongly recommended.

The sending of confidential material in the form of PDFs or any other format, via any means outside of the system (email, SMS etc) is not secure and is not recommended unless appropriate security measures have been put in place.

Reviewing PDFs Documents

The forms that are generated by Quantum have been thoroughly tested and checked for consistency with the official HMC forms. However, it is very important that forms generated to pdf for submission to court should be checked and reviewed prior to being submitted as Class Legal cannot be held responsible for the legal validity of the forms due to errors or omissions from any cause.