

PE2185/C: Introduce stronger safeguards around the use of digital material in court proceedings

Willie Coffey MSP written submission, 24 November 2025

The Scottish Government is supporting the development and roll-out of a system for sharing digital evidence in criminal cases.

Digital Evidence Sharing Capability (DESC) allows police officers, prosecutors, defence lawyers, court staff and judges to access a secure, unified system to collect, store, process and manage evidence digitally. As noted in the SPICe briefing:

The DESC was highlighted in the Policy Memorandum published along with the Criminal Justice Modernisation and Abusive Domestic Behaviour Reviews (Scotland) Bill (passed on 7 October 2025). It noted that:

“Through DESC, digital evidence, such as photographs or video footage, can be shared by members of the public at the point of reporting a crime to the police. This evidence is then shared with the prosecution and the defence agent for the accused in order to allow early consideration and possible resolution of cases.” (para 64)

The DESC is designed with features intended to preserve the integrity of evidence once it is entered into the system. The above Policy Memorandum stated that:

“assurance can be provided through its automatic audit function which shows every activity on the uploaded file from its receipt to the conclusion of the case”. (para 72)

However, these features are not aimed at checking the reliability of digital evidence prior to it being entered into the system.

Further, it is important that with the advent of AI and the ability to produce false digital content which is indistinguishable from genuine and authentic material that clear measures are put in place to help prevent this.

In that regard, I respectfully ask in support of my constituent, that all digital material presented in court be assessed, and verified as reliable prior to it being entered into the system.

I therefore support the key aim of Petition 2185 that this gap be addressed by introducing a clear, preventative safeguard requiring that all digital evidence be verifiably sourced, time-stamped, and authenticated before it can be used in court proceedings or relied upon during investigation.