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

## Petitioner written submission, 8 November 2025

Thank you for taking the time to consider my response.

**The Scottish Government response**

I must express that the Scottish Government's reply to my petition has missed the heart of the issue I raised. This is not simply a matter of what happens in the courtroom; it is about the long, painful months that innocent people can endure before they ever have a chance to defend themselves.

In my own experience, I spent nine agonising months under the weight of false allegations. During that time, I was subjected to public humiliation, constant fear, and even death threats from strangers who believed the accusations. My accuser was free to spread misinformation online while I was silenced by bail conditions, unable to share my side of the story. I lost my belongings, my reputation was attacked, and I came perilously close to ending my own life because of the unbearable stress.

The point of my petition is simple but crucial: before digital evidence is ever used to drag someone through the court system, it must be thoroughly investigated at the very start. In an age where digital manipulation is easy and evidence can be fabricated in moments, we cannot afford to wait until a trial date to discover the truth.

This is about the police doing their job and making those simple checks that we all know are necessary in this digital age. It is frankly unreasonable that these checks are not already standard procedure, because anyone can edit or fabricate evidence on a smartphone. Law enforcement and judicial authorities are well aware of these risks, and yet there remains no formal safeguard to ensure that such material is properly verified before it is acted upon. My petition simply asks that police thoroughly investigate digital evidence before it ever reaches a courtroom so that no innocent person has to endure what I went through.

I would also like to note that I currently have a police complaint still outstanding since May 2025, in which I have pointed out that a simple investigation by the police would have prevented this entire situation. It has since been demonstrated that false digital evidence was provided to the police, something that would have been detected through proper investigation. The second part of my complaint is that I am asking the authorities to now investigate this and hold the individual responsible to account. Yet as of November, I still have not received an answer.

I urge you to see that this is not about adding unnecessary hurdles, but about protecting innocent lives from being upended by unverified accusations. A simple check at the outset would have spared me and many others months of suffering. I hope you will take this into serious consideration so that no one else has to endure what I went through.

Thank you for your understanding and for addressing the true heart of this petition.

**The SPICe briefing**

I would like to thank the Scottish Parliament Information Centre (SPICe) for preparing such a clear and balanced briefing to accompany my petition. The paper highlights the key issues surrounding the handling and reliability of digital evidence, and I would like to offer the following short response for clarification and context.

The briefing correctly notes that there is currently no legislative requirement specifying how digital material must be verified prior to its use as evidence. This is the central issue my petition seeks to address. At present, digital evidence can be presented and acted upon long before it has been authenticated, verified, or linked to a verifiable source. This gap in legislation has serious implications for both justice and fairness.

While I welcome the development of the Digital Evidence Sharing Capability (DESC) system, as highlighted in the SPICe paper, it is important to note that DESC is primarily concerned with secure storage and sharing. It does not verify authenticity at the point of upload. In other words, DESC ensures that evidence is handled securely after it has been gathered, but it does not ensure that what is being uploaded is genuine or unaltered in the first place.

Similarly, the Crown Office and Procurator Fiscal Service (COPFS) guidance referenced in the briefing describes a process in which “provenance must be proven before evidence attains evidential status,” and that any disputes can be resolved in court. The problem with this approach is timing. These checks and disputes take place after a person has been charged or brought to trial, meaning that individuals can be subjected to lengthy investigations and restrictions based on unverified or fabricated digital material.

The SPICe briefing also mentions the Criminal Justice Modernisation and Abusive Domestic Behaviour Reviews (Scotland) Bill, which introduces provisions for digital evidence audits. However, as the paper accurately points out, these audits concern data handling and retention, not authentication or verification. They do not prevent false or manipulated evidence from entering the process in the first place.

For these reasons, I respectfully submit that the gap identified by SPICe represents a genuine weakness in the current justice framework. My petition simply asks 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.

I would again like to thank SPICe and the Committee for their consideration of this issue. It is my sincere hope that this petition will prompt a wider discussion on how Scotland can lead by example in ensuring the integrity of digital evidence and protecting both victims and the wrongly accused alike.