

Digital Evidence Preservation Guide

Immediate steps for devices, files, accounts and communications.

Preserve the source

Do not reset, update, delete, rename, forward or open files unnecessarily. Preserve original devices and native files.

Record where the item came from, who possessed it and any actions already taken.

Create separation

Keep original evidence separate from working copies. Where possible, use a forensic acquisition or verified duplicate for examination.

Record context

Note dates, persons, phone numbers, email addresses, account names, passwords/PIN availability and the question the evidence must answer.

Quick checklist

	Action
	Stop unnecessary use of relevant devices
	Photograph device state and connections
	Retain chargers, cables and peripherals
	Preserve native files and full message exports
	Record every transfer or action
	Arrange secure transfer with the examiner

Important: This guide is general information and does not replace matter-specific legal advice or forensic direction. Do not send original evidence through ordinary email or messaging applications unless secure transfer arrangements have been agreed.