1.0 Summary of Changes

1.1 On its review, the following changes have been made to this policy:

- Two new paragraphs added as 3.1 and 3.2 giving an explanation of accreditation and digital forensics;
- Within Section 4.3 the 9 protected EIA characteristic have been updated;
- New paragraphs added within section 7 regarding data security and retention and disposal of records.

2.0 What this Policy is about

2.1 The purpose of this document is to provide direction to operational officers and staff on the seizure, handling and submission of items for examination by the Digital Forensic Unit (DFU). This includes computers and related devices as well as mobile phones and CCTV recorded by third parties.

2.2 It is the responsibility of the officer in charge (OIC) of any investigation to ensure compliance with this policy, legislation and, in particular, to be sure that the procedures/SOPs adopted in the seizure of any property is done in accordance with statute and current case law.

Compliance with this policy and any linked procedures/SOPs is mandatory.

3.0 Statement of Policy

3.1 The Forensic Science Regulator (FSR) expects digital forensic activities performed by Essex Police and Kent Police to be conducted to the FSR’s Code of Practice and Conduct and be accredited to ISO 17025 (general requirements for the competence of testing and calibration laboratories):

- Essex Police and Kent Police current schedule of accreditation

3.2 Digital forensics is the process by which information is extracted from data storage media (e.g., devices, remote storage and systems associated with computing, imaging, image comparison, video processing and enhancement [including CCTV], audio analysis, satellite navigation, communications), rendered into a useable form, processed and interpreted for the purpose of obtaining intelligence for use in investigations, or evidence for use in criminal proceedings.

3.3 Digital evidence has become an integral part of many investigations and in numerous cases has resulted in crucial evidence being produced. It is therefore essential that this evidential source is not rendered ineffective due to it either being corrupted or its validity being brought into question by actions taken by officers and staff.
3.4 It is therefore essential that officers and staff interact with the device(s) in question as little as possible (with the exception of CCTV) to prevent any inadvertent changes being made to the material of interest or any other material present. The DFU will always try and accommodate legitimate requests for urgent work negating the need for ad-hoc examination at premises or police stations.

3.5 It is equally important that all items submitted for analysis have been correctly handled during seizure and transportation and that they have been accurately documented.

3.6 The connected procedures/Standard Operating Procedures (SOPs) provide instruction on how this volatile evidential source is to be handled. This policy and accompanying procedures/SOPs comply with the recommendations detailed in the ACPO Good Practice Guide on Digital Evidence (See ‘Other source documents’, below).

3.7 The Counter Terrorism and Security Act (CTSA) 2015 places a duty on various specified authorities to have ‘due regard to the need to prevent people being drawn into terrorism’. This is referred to as a ‘Prevent Duty’ and involves:

- Responding to the ideological challenge of terrorism;
- Preventing people from being drawn into terrorism;
- Working with sectors and institutions where there are risks of radicalisation.

3.7.1 The CTSA 2015 also places a duty upon specified authorities in relation to supporting people vulnerable to being drawn into terrorism through the Channel programme. Channel is a multi-agency safeguarding programme, which provides support to those individuals who may be vulnerable to being drawn into any form of extremism that could lead to terrorist related activity.

3.7.2 This policy has been reviewed and assessed that the CTSA duties could be relevant and as such your attention is drawn to your responsibilities under the Act. Further details about the Prevent Duty and the Channel Duty can be found below.

- Learn more about the Prevent Duty.
- Learn more about the Channel Duty

4.0 Implications of the Policy

4.1 Finance / Staffing / Training / Other

4.1.1 No financial or staffing implications have been identified in the creation of this policy.
4.2 Risk Assessment(s)

4.2.1 This policy has been assessed as medium risk.

4.3 Equality Impact Assessment

4.3.1 An Equality Impact Assessment has been carried out and shows the proposals in this procedure would have no potential or actual differential impact on grounds of age, sex, disability, race, religion or belief, marriage and civil partnership, sexual orientation, gender reassignment and pregnancy and maternity.

5.0 Consultation

5.1 The following have been consulted during the formulation of this document:

- Serious and Organised Crime Unit;
- Human Resources;
- Estates;
- IT Security;
- Finance;
- Legal
- Freedom of Information
- Health and Safety;
- Equality and Diversity

6.0 Monitoring and Review

6.1 This policy and its attendant procedures/SOPs will be monitored by, or on behalf of, the Head of the Serious Crime Directorate to ensure that they remain accurate and compliant with both legislation and national/local drivers.

6.2 This policy and its attendant procedures/SOP will be reviewed every 2 years by, or on behalf of, the Head of the Serious Crime Directorate to ensure that it is accurate and fit for purpose.

6.3 Performance data for digital forensic work is published on a monthly basis.

7.0 Related force policies or related procedures (Essex) / linked standard operating procedures (Kent)

- S 3001 Procedure/SOP - Digital Evidence - Computers
- S 3002 Procedure/SOP - Digital Evidence - Mobile Phones
- S 3004 Procedure/SOP - Digital Evidence - CCTV
- S 3005 Procedure/SOP - Digital Evidence – Property Disposal
7.1 Data Security

7.1.1 Essex Police and Kent Police have measures in place to protect the security of your data in accordance with our Information Management Policy – W1000 Policy – Information Management.

7.2 Retention & Disposal of Records


7.2.2 We will only hold data for as long as necessary for the purposes for which we collected.

8.0 Other source documents, e.g., Legislation, APP, partnership agreements (if applicable)

- ACPO Good Practice Guide for Digital Evidence