Force Policy & Procedure:	**Installation, Monitoring and Data Compliance for Force Owned Closed Circuit Television (CCTV)**
Reference Number:	**D011**
Policy Version Date:	**24 September 2021**
Review Date:	**24 September 2022**
Policy Ownership:	**Prevention Department**
Portfolio Holder:	**Assistant Chief Constable Local Policing and Connectivity**

Contents:

1. Policy Statement [FOIA Open]

1.1 Devon and Cornwall Police aims, by working in partnership with other agencies, to bring about safer communities, reduce disorder, crime and the fear of crime and to contribute to the delivery of justice in a way which secures and maintains public confidence. The policing of Devon, Cornwall and the Isles of Scilly will focus on bringing the police and the community together in the fight against crime.

1.2 As part of this aim the Force is committed to the protection of life and property and the protection of vulnerable communities whilst preserving the rights of individuals. In pursuit of these commitments Devon & Cornwall Police is committed to using CCTV to prevent and detect crime and protect the rights of individuals across its estate.

1.3 In the application of this policy staff are reminded of the need to comply with the standards and principles of the Code of Ethics for policing.

2. Introduction [FOIA Open]

2.1 This policy only refers to CCTV systems which are owned by the Police and Crime Commissioner (PCC) for Devon and Cornwall. The Data Controller for the system is the Chief Constable.

2.2 The Force will only install CCTV and process data to assist with:
- The safety and security of all persons on police premises, police buildings and assets (not to be used for staff discipline).
- The gathering of data and intelligence to assist with the detection and prevention of all crimes,
- Provide data to assist with the apprehension and prosecution of offenders.

2.3 All Force CCTV system installation and operating codes must be fully compliant with appropriate legislation;

- Human Rights Act 1998
- Data Protection Act 2018.
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Information Commissioners Office - CCTV Code of Practice (v 1.2)
- Information Commissioners Office - Guide to the General Data Protection Regulation [GDPR] (May 2018)
- Surveillance Camera Commissioner - GOV.UK

2.4 The installation of CCTV by the Force must fit within the reasons outlined in paragraph 2.2 of this document and be compliant with the legislation outlined at 2.3 above.

2.5 The data produced and stored by the Force CCTV system is: lawfully compliant with the requirements of the Information Commissioner's Office (ICO), is secure, of evidential quality and its continuity can be proven.

2.6 When considering the installation, monitoring of Force CCTV and the storage of data the following must be considered/consulted:
- Contracts Officer, Procurement Department.
- Alliance Data Protection Team, Alliance Information Management Department, SA045 (Data Protection).
- Covert Authorisations Bureau, D232 (Compliance and Procedures for Covert Policy Activity).
- Video Processing Unit Supervisor, Criminal Justice Department.
- Counter Terrorism Support Advisor, Crime Prevention Officer (CPO) and Designing Out Crime Officer (DOCO)

2.7 The installation of Force CCTV must be lawful, data compliant, fit for purpose, producing high quality evidential images that will support the judicial process. A responsible person must be identified for the ongoing local upkeep of camera locations e.g. lens kept clean, view not obscured by subsequent growth of foliage or new building works etc.

3. Procedures [FOIA Open]

3.1 Prior to considering the installation of a Force CCTV system the Surveillance Camera Commissioner - “Passport to Compliance” documentation must be completed. This documentation outlines the requirements that are to be considered, with guidance about the principles and necessary stages when planning, implementing and operating a surveillance camera system to ensure it complies with the code.

3.2 Should the Surveillance Camera Commissioner - “Passport to Compliance” process identify that the desired problem cannot be solved nor the expected solution obtained, then the installation should be abandoned.

4. Assessment Compliance [FOIA Open]

4.1 This policy has been drafted and audited to comply with the principles of the Human Rights Act. Equality and diversity issues have also been considered to ensure compliance with Equality legislation and policies. In addition, Data Protection, Freedom of Information, Management of Police Information and Health and Safety issues have been considered. Adherence to this document will therefore ensure compliance with all relevant legislation, Code of Ethics and other appropriate internal policies.

5. Review and Ownership [FOIA Open]

5.1 The review of the contents of this policy is the responsibility of the Prevention Department. Review of the policy will be undertaken annually in consultation with the stakeholders as listed below

- Building and Estates
- Information Management Department
- Legal Services
- Prevention Department (D&C)

6. Useful Links [FOIA Open]

6.1 This policy should be read in conjunction with policies:
SA045 – Alliance Data Protection Policy
D124 – Surveillance
D206 – Closed Circuit Television – Ports (CCTV)
D232 – Compliance & Procedures for Covert Policing Activity

Information Commissioners Office - CCTV Code of Practice (v 1.2)
Surveillance Camera Commissioner - “Passport to Compliance” (November 2018)
Information Commissioners Office - Guide to the General Data Protection Regulation [GDPR] (May 2018)
Surveillance Camera Commissioner