



# COTSWOLD DISTRICT COUNCIL

Council name	<b>COTSWOLD DISTRICT COUNCIL</b>
Name and date of Committee	<b>CABINET - 6<sup>TH</sup> JANUARY 2020</b>
Report Number	<b>AGENDA ITEM (8)</b>
Subject	<b>CCTV POLICY</b>
Wards affected	ALL
Accountable member	Cllr. Jenny Forde - Cabinet Member for Health, Well-being and Public Safety Email: <a href="mailto:jenny.forde@cotswold.gov.uk">jenny.forde@cotswold.gov.uk</a>
Accountable officer	Claire Hughes - Business Manager for Corporate Responsibility Tel: 01594 812515 Email: <a href="mailto:claire.hughes@publicagroup.uk">claire.hughes@publicagroup.uk</a>
Summary/Purpose	To seek approval of a CCTV policy which will govern the operation of CCTV operated by the Council as a data controller.
Annexes	Annex A
Recommendation/s	<i>That Cabinet:</i> <i>a) Approves the CCTV Policy;</i> <i>b) Notes that the policy will be effective immediately.</i>
Corporate priorities	Provide high quality services at the lowest possible cost to Council Taxpayers.
Key Decision	NO
Exempt	NO
Consultees/ Consultation	Cabinet Members Senior Officers

## **1. BACKGROUND**

- 1.1.** In recent years, there has been a substantial increase in the number of Closed Circuit Television Cameras nationally. This is driven in part by a reduction in the costs of installing and operating this type of equipment. This increase has coincided with heightened privacy concerns, which have resulted in laws, regulations and codes of practice designed to ensure that the use of cameras is legitimate, proportionate to the intended purpose and respectful of legitimate privacy expectations. Article 8 of the Human Rights Convention recognises the right to a private and family life. Where CCTV captures images of people which comprise personal data, there is potential for this to infringe on the privacy of individuals. Accordingly, there is an obligation for CCTV installations and handling practices to comply with the 3rd Data Protection Principle (data minimisation) as well as the 6th Principle (Appropriate technical and organisational security) as set out in the Data Protection Act and General Data Protection Regulations.
- 1.2.** The Council operates CCTV systems as a proportionate response to identified problems, insofar as it is considered necessary in a democratic society in the interests of public safety, for the prevention and detection of crime and disorder, and for the protection of the rights and freedoms of others.
- 1.3.** The Information Commissioner's Office ('the ICO') has enforcement powers which include the power to issue directives to remove or modify CCTV installations. The ICO is supported by the Surveillance Camera Commissioner, who was established under the Protection of Freedoms Act 2012 and he has issued codes of practice for the use of these cameras, which include guiding principles.

## **2. MAIN POINTS**

- 2.1.** The Council acts as data controller for the CCTV systems it operates for the purposes of preventing and detecting crime and for ensuring public safety.
- 2.2.** Some staff or contractors with public enforcement roles wear body-mounted cameras to protect their safety and wellbeing whilst carrying out their duties.
- 2.3.** As a data controller, the Council is obliged to comply with all relevant legislation and the codes of practice issued by the Surveillance Camera Commissioner. The Council is also subject to inspections.
- 2.4.** A key part of the Surveillance Camera Commissioner's Code of Practice and something upon which the Council may be inspected is the requirement to have a fully documented CCTV Policy. The purpose of this policy is, therefore, to fulfil that requirement and to ensure that the Council is acting lawfully.
- 2.5.** The policy will be supplemented with an operators guide which will provide detailed guidance for those operating the CCTV, including guidance on reviewing footage. A comprehensive register of all CCTV cameras has also been established.

## **3. FINANCIAL IMPLICATIONS**

- 3.1.** There are no direct financial implications as a result of this policy but failure to comply with the legislation and codes of practice could result in the Council being fined.

#### **4. LEGAL IMPLICATIONS**

- 4.1. Failure to adopt the policy may result in the Council being in breach of relevant legislation, specifically the Data Protection Act 2018 and the Protection of Freedoms Act 2012.

#### **5. RISK ASSESSMENT**

- 5.1. The Council risks being fined if it fails to comply with the relevant legislation. There is also a significant reputational risk if the Council is not controlling and monitoring the use of CCTV effectively.

#### **6. EQUALITIES IMPACT**

- 6.1. There are no specific equalities impacts as a result of adopting this policy. However, the installation of CCTV cameras requires the completion of a privacy impact assessment which would highlight any equalities issues. A privacy impact assessment has been completed for all CCTV operated by Cotswold District Council.

#### **7. ALTERNATIVE OPTIONS**

- 7.1. The Council could choose not to adopt the policy but would be opening itself up to significant risks so this is not recommended.

#### **8. BACKGROUND PAPERS**

- 8.1. None

(END)