

CCTV policy

1. Introduction

1.1 This policy forms part of the information security policy. Its purpose is to ensure we comply with legal requirements for CCTV use.

2. Legal compliance

2.1 Any surveillance cameras capture personal data, so the use of CCTV has data protection and privacy implications. We must comply with the Information Commissioner's Office [code of practice](#) and relevant legislation including the Data Protection Act 1998 (DPA) and Human Rights Act 1998.

2.2 The Surveillance Camera Code of Practice in the Protection of Freedoms Act 2012 contains 12 guiding principles, which are referenced in the ICO code.

3. Policy statement

3.1 We use CCTV at the Caltec Group to support the safety and security of our staff and premises. It will be used to:

- act as a deterrent to intruders and to the theft or misuse of property or information
- act as a deterrent to improper or aggressive behaviour
- to provide evidence to support the investigation of safety- and security-related incidents

3.2 We will not use CCTV for other purposes and will not include audio recording.

3.3 CCTV cameras will be sited so that recordings meet the stated purposes. They will cover entrances to the premises and offices, the evidence room, secure storage area and Workshop and yard.

3.4 We will be transparent in our use of CCTV and we will make all who use the premises aware of its use through appropriate signs and information about our policy.

3.5 We will have procedures for operating and accessing CCTV recording equipment, which we will communicate to those staff, contractors and third parties who administer, access or operate the equipment or data.

3.6 CCTV recordings and data will be classified as confidential information and held in systems with appropriate security measures to safeguard against unauthorised access and use.

3.7 We will ensure that contractual arrangements with any contractors or third party suppliers who may maintain or administer CCTV systems on our behalf cover confidentiality and information security.

3.8 Users will only access and view CCTV recordings and data in response to a request authorised by the head of governance or a member of the Senior Leadership Group.

3.9 Access to CCTV systems, recordings and data for the purposes of maintenance or support will be restricted to users authorised by the head of IT and facilities.

3.10 Information will be stored in a way that allows relevant frames to be isolated to answer a request.

3.11 CCTV information will not be disclosed except as necessary for the stated purpose or to respond lawfully to a request under the DPA or Freedom of Information Act (FOI).

3.12 Recordings and data will routinely be held for 3 months and then deleted.

CCTV policy