

# WINSLOW TOWN COUNCIL



## CCTV Policy

### Introduction

This Policy is to control the management of the Town Council's CCTV system. It takes due account of the Code of Practice '*In the picture: A data protection code of practice for surveillance cameras and personal information*' published by the Information Commissioner's Office (May 2015, the '*ICO Code*') and the '*Surveillance Camera Code of Practice*' published by the Home Office (2013, the '*PoFA Code*') and will be subject to periodic review by WTC to reflect any legislative changes.

### **The Town Council accepts the Data Protection Principles set out in the Data Protection Act 1998:**

- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under this Act.
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

### **The Town Council accepts the guiding principles of the Surveillance Camera Code of Conduct:**

- Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
- The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
- There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.
- There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
- Personal Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
- No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
- Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

- Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
- Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
- There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
- When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.
- Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

### **Statement of Purpose**

The Town Council wishes to protect the Council's assets including its staff.

### **Storage and Handling of Data**

Access to data captured by the CCTV system is limited to Town Council employees, the Town Council's authorised CCTV contractor and for purposes of assisting community policing Thames Valley Police.

No images shall be shared with or viewed by third parties other than:

- law enforcement agencies, and
- other persons entitled by law (e.g. via subject access requests or freedom of information requests).

A procedure to control the storage and handling of data shall be authorised and maintained by the Amenities Committee.

### **Personal Information**

Any individual whose image is captured on the CCTV system may request a copy of their personal data subject to payment of a fee.

A procedure governing such 'subject access requests' shall be authorised and maintained by the Amenities Committee.

Freedom of Information requests relating to CCTV images will be handled under the Town Council's existing policy while remaining within the guiding principles set out at the start of this policy.

### **Privacy**

The use of a CCTV system affects the privacy of individuals and must therefore be justified. The Town Council records its justification in a Privacy Impact Assessment.

### **Annual Review**

At the end of each calendar year the Clerk shall compile for the Amenities Committee a report on the use of the CCTV system, any subject access requests, breaches of this policy and any other relevant learning.

Prior to the Annual Council Meeting, and informed by the Clerk's report, the Amenities Committee shall prepare a Privacy Impact Assessment for the forthcoming Council year. In light of the Privacy Impact Assessment and any changes to the regulatory framework the Amenities Committee shall make a recommendation to Council on whether the use of CCTV is justified and if so what (if any) changes are required to the system.

The Town Council shall consider the recommendation of the Amenities Committee and decide at the Annual Council Meeting whether to authorise the use of CCTV for the forthcoming year and if so what changes should be made.

In the event that the Town Council fails to authorise the use of the CCTV system it will be deactivated at the earliest practicable date.

## **Signage**

Signage is a major contributor to the deterrent effect of CCTV system. In addition, the ICO Code requires that people are warned by prominent signage when they are in an area that is under surveillance. Signs are therefore to be placed (where practicable) at all entry points into areas covered by CCTV, with additional signs where necessary within the covered areas. The signs shall include:

- the Town Council's name and address, and
- the purpose of the CCTV system.

## **Overall Responsibility**

Winslow Town Council is the Data Controller for purposes of the Data Protection Act 1998 and retains overall responsibility for the scheme.

## **Management of the System**

Day-to-day responsibility for all aspects of the CCTV system rests with the Clerk to the Council who should be the first point of contact for all enquiries.

All internal procedures required for the operation and management of the CCTV system may be implemented at the Clerk's discretion.

**V24.1**

**Reviewed 16/05/2024**