PITSTONE PARISH COUNCIL

CCTV Policy and Privacy Impact Risk Assessment

1. Managing the Policy

1.1. Compliance

This policy applies to all staff, whether permanent or temporary, Members and contractors.

1.2. Advice and Training

If you do not understand anything in this policy or feel you need specific training to comply with it, you should bring this to the attention of your manager.

1.3. Equality and Diversity

Every policy must consider equality and identify any potential barriers or discrimination faced by people protected by equality legislation.

2. INTRODUCTION

This policy sets out how the parish council will operate and maintain CCTV at our premises.

The only CCTV operated by the parish council is via fixed cameras located at the pavilion site. The parish council does not operate any remote, mobile, or on-body CCTV systems.

3. PURPOSE AND OBJECTIVES

The purpose of this policy is to ensure the management, operation and use of CCTV is regulated to ensure consistency and compliance with relevant legislation.

The Policy considers the:

- Surveillance Camera Code of Practice (Nov 21) and associated guidance from the Surveillance Camera Commissioner
- CCTV Code of Practice issued by the Information Commissioner's Office (ICO)
- Requirements for processing personal data as set out in the General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Right to privacy as set out in Article 8 of the Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Crime and Disorder Act 1998

All associated information, documents and recordings obtained by CCTV must be held and used in accordance with data protection legislation, the ICO's CCTV Code of Practice and the Surveillance Camera Code of Practice.

Images obtained from CCTV recordings will not be used for any commercial purpose.

Recordings will only be released to the media for use in an investigation of a crime provided the written consent of the Police has been given. Recordings will not be released to the media for entertainment purposes.

Archived CCTV images will not be kept for longer than is necessary for the purpose of Police or council evidence. Images no longer required will be securely disposed of and such disposal will be recorded on the council's Disposal Log.

4. ROLES AND RESPONSIBILITIES

This section sets out the roles and responsibilities of staff in relation to the effective operation of CCTV.

The full parish council and parish clerk are responsible for ensuring compliance with the policy in relation to all CCTV operated by the parish council and for ensuring compliance with the GDPR, Data Protection Act and Regulation of Investigatory Powers Act in relation to the processing of images and the use of any covert CCTV.

Only the parish clerk & assistant, facilities manager and chairman of the council can access our CCTV footage.

All staff, including temporary and contractors, and Members are responsible for complying with this policy.

The council is a Data Controller for the purposes of data protection legislation.

5. USE OF CCTV IN THE PARISH

Predominantly the council will use CCTV for the purpose of reducing and detecting crime and anti-social behaviour as well as ensuring the health and safety of the public and its staff.

The use of CCTV at parish council locations should always be for a specific purpose and clear signage indicating CCTV is in operation will be provided in a prominent place.

CCTV at council premises may also be used for the purpose of staff training and in relation to disciplinary matters where necessary.

6. OPERATION

CCTV at the pavilion may be subject to live monitoring from the site office or remotely. Images may also be recorded but not monitored in real time.

Images are recorded and retained for up to 31 days unless they are required for an ongoing investigation. Where footage is required for an investigation a copy will be held for up to one year, or such other period as may be necessary to progress the investigation.

Recorded information is held on digital recorders or in secure computer files with access restricted to nominated council staff.

Recorded images will only be viewed from the council office or via remote access locations with restricted access.

All requests to access or view recorded images should be made to Pitstone Parish Council.

All access to CCTV images will be logged on the appropriate form in the CCTV Log Book.

All requests for access to recorded images must be logged. This applies to requests from members of staff or third parties, for example, the Police. Requests from individuals for a copy of their personal data, including recorded images, will be considered as a subject access request under the GDPR. Section 7, below, relates to such requests.

To ensure the preservation of images for evidential purposes, the following will apply:

- DVD/USBs must be identified by a Name, Date, Time, Camera Location and Recording equipment used.
- The DVD/USB must be signed by the person who downloaded the images, dated, witnessed, and stored in a sealed envelope.
- An original copy of the image downloaded must be retained, date stamped and stored in a secure area.
- The log must be completed detailing the release of the DVD/USB to the Police, council department (or another agency if appropriate)
- If a DVD/USB is required as evidence, a copy may be released to the Police, who will become the Data Controller and, therefore, responsible for the images.
- The Police may require the council to retain stored DVD/USBs for possible future evidence. Such DVD/USBs will be indexed and securely stored for a period of 1 year, at which point they will be securely destroyed.
- Applications received from external agencies (for example solicitors or insurance companies) to view recordings must in the first instance be made via the parish council. If appropriate, images may be downloaded to DVD/USB and released where satisfactory documentary evidence is produced confirming legal proceedings, or in response to a Court Order. A charge may apply for insurance companies.

It should be noted that, where it is necessary to download images onto removable media (DVD/USB) they will be unencrypted to allow viewing by third parties. A suitable method to ensure the secure transfer of the removable media must be used and documented.

Still photographs of CCTV images must not be taken as a matter of routine. The taking of each photograph must be capable of justification (for example for the prevention or detection of crime and anti-social behaviour) and only done so with the permission from the immediate person in charge of the CCTV system.

7. SUBJECT ACCESS REQUESTS

The GDPR provides individuals with the right to access a copy of their personal data held by the council. This includes the right to access a copy of CCTV images. You will need to specify an exact date & time and to provide proof of your identity. For guidance, please see the https://www.gov.uk/request-cctv-footage-of-yourself

Subject access requests should be forwarded to the parish clerk for processing and you will be provided with a Subject Access Request form for completion.

8. FREEDOM OF INFORMATION

As a public authority, the council may receive requests for a copy of recorded information under the Freedom of Information Act 2000 (FOI). If a request for a copy of a CCTV recording is made the following will be considered:

- Is the information the personal data of the requester? If so, disclosure is exempt under FOI, but the request will be considered as a subject access request under the GDPR.
- Is the information the personal data of individuals other than the requester? If so, it is likely to fall under the exemption for personal data unless disclosure would not breach the GDPR principles.

Requests may also be received regarding the CCTV itself – for example, the siting and operation of cameras or the costs associated with using and maintaining them.

Information following such a request would be released unless a valid exemption applied.

All requests made under FOI should be referred to the parish clerk.

9. REVIEW

All uses of CCTV should be reviewed on an annual basis to ensure:

- There is still a legitimate reason to maintain the CCTV.
- The CCTV cameras continue to provide images of sufficient quality.
- Signage remains up to date and relevant.

If it is determined additional cameras are necessary, either to supplement existing CCTV or to cover another area, a Data Protection Impact Assessment (DPIA) must be completed.

The Surveillance Camera Commissioner has provided a data protection impact assessment for surveillance camera systems https://www.gov.uk/government/publications/data-protection-impactassessments-for-surveillance-cameras which must be completed whenever any changes to a system are being considered, including adding or removing cameras, changes to location and system upgrades.

10. SURVEILLANCE CAMERA CODE OF PRACTICE

The Surveillance Camera Code of Practice was issued in 2013 following the introduction of the Protection of Freedoms Act 2012 and further updated in 2014. The Code provides guidance on the appropriate and effective use of surveillance camera systems.

The council is a relevant authority as defined by Section 33 of the Protection of Freedoms Act and, therefore, must have regard to the code.

The code applies to the use of surveillance camera systems that operate in public places, regardless of whether there is any live viewing or recording of images or information or associated data.

The code provides 12 guiding principles which the council has adopted. These are:

- 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 consider 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.
- 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.

This policy was adopted by Pitstone Parish Council on …11/4/24……..… Minute Ref: ……. ……SL7/24.11……

and will be reviewed at least annually.

K Weber

_____

Chairman