Parish Clerk - Mrs Sara Archer, 204 Acol Street, Acol, Ramsgate, Kent, CT12 4JN
Tel: 01843 821989 Email: clerk@acolparishcouncil.org.uk

CCTV POLICY

Reviewed – 17.04.25

1. Introduction

This Policy is to control the management, operation, use and confidentiality of the CCTV systems in the Parish. This policy was prepared after taking due account of the Code of Practice published by the Data Protection Commissioner (revised 2008), and the 2013 Surveillance Camera Code of Practice guidelines following the introduction of the Protection of Freedoms Act 2012. This policy will be subject to periodic review by the Parish Council to ensure that it continues to reflect the public interest and that it and the system meets all legislative requirements.

2. Statement of Purpose

To provide a safe and secure environment for the benefit of those who might visit, work or live in the area. The system will not be used to invade the privacy of any individual, except when carried out in accordance with the law. The scheme will be used for the following purposes:

• to reduce the fear of crime by persons within the parish, so they can enter and leave buildings and use facilities without fear of intimidation by individuals or groups

• to reduce the vandalism of property and to prevent, deter and detect crime and disorder

• to assist the police, the Parish Council and other Law Enforcement Agencies with identification, detection, apprehension and prosecution of offenders by examining and using retrievable evidence relating to crime, public order or contravention of bye-laws

• to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited in the Parish that are not hidden and signs on display.

• to assist all “emergency services” to carry out their lawful duties.

Static cameras enable this purpose.

3. Legal Framework and Requirements

Acol Parish Council accepts that the General Data Protection Regulations (2018) has several underlying principles. These include that personal data:

• Must be processed lawfully, fairly and transparently.

• Is only used for a specific processing purpose that the data subject has been made aware of and no other, without further consent.

• Should be adequate, relevant and limited i.e. only the minimum amount of data should be kept for specific processing.

• Must be accurate and where necessary kept up to date.

• Should not be stored for longer than is necessary, and that storage is safe and secure.

• Should be processed in a manner that ensures appropriate security and protection. Acol Parish Council recognises the key changes to legislation concerning data protection in relation to the General Data Protection Regulations (2018) are:

• Changes to how consent can be obtained from data subjects for the use of their data. For example, data subjects have to explicitly ‘opt in’ to allowing their data to be shared, and it must be made clear for what purpose their data is being used.

• Data subjects have new rights, such as data portability and the right to be forgotten.

• Data must only be used for the purpose it was gathered for and should be deleted when it is no longer needed for that purpose.

• Sanctions over sharing data outside the European Economic Area (“EEA”) will be strengthened. This requires councils to ensure appropriate privacy safeguards are in place with organisations (e.g. a business hosting and maintaining the council’s server) holding data outside the EEA or that the ‘importer’ of data is on a list of countries which the European Union has deemed to have adequate protection for citizens regarding data protection.

• All councillors, Parish Clerk and other relevant staff must have suitable training and awareness as well as additional sources of guidance and support when required.

• Conducting Data Protection Impact Assessments (DPIAs) in order to design data privacy into any new systems and processes will often be mandatory e.g. if new technology is deployed, where there is processing on a large scale of 'sensitive personal data', or if profiling is performed which will have an impact on individuals.
• Councils and parish meetings can choose to appoint a Data Protection Officer.
• Data breaches must be reported (where this is required) to the ICO within 72 hours of the breach.
• A new principle of accountability puts the compliance burden on councils, requiring them to produce and maintain documents that demonstrate what actions have been taken to achieve compliance.

Acol Parish Council recognises the guidelines in the 2013 Home Office Code of Practice:
• 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.
• 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. (access log held at Council offices) • 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.

4. Our Policy

1. To inform all who come into the Village that CCTV is in use.

2. To ensure the prevention of intrusion of privacy for immediate neighbours.

3. To keep images from CCTV secure and controlled by authorised personnel.

4. To maintain all CCTV equipment in working order.

5. The Chair/Clerk will be able to view the live image display and be able to review/access recorded images to achieve the stated purpose.

6. Within the purpose of the CCTV system such images may be shared with the Police enforcement agency if deemed necessary by the Chair/Clerk.

7. The picture quality maintenance and service of equipment will be carried out by the installation company and a monthly check will take place by Chair/Clerk.

8. The images will be digitally recorded on a rolling programme of 31 days. Unless required for evidence purposes, this retention will automatically overwrite the oldest images.

9. Any retention of images kept on the server will be kept until they are no longer required then overwritten in the normal way.

10. Any downloaded images can only be made with the Chair/Clerk's consent to a digital disc and to be only made available to those who are responsible to achieve the stated legitimate purpose.

11. All copies of downloaded images will be catalogued. These images will be destroyed after they are no longer required. Verified written proof will be retained as confirmation of destruction.

12. Any request to access images from our system from third party groups will be dealt with accordingly by the Chair/Clerk.

5. Disclosure of Images

Disclosure of images from the CCTV system must be controlled and consistent with the purpose for which the system was established. For example, if the system is established to help prevent and detect crime it will be appropriate to disclose images to authorised law enforcement agencies where a crime needs to be investigated.

Any other person or organisation wishing to view images must be referred to the Clerk or Chairman of the Parish Council and must be made in writing. In all such cases a consideration will be made about the duties under the General Data Protection Regulations and whether this duty would be breached by releasing the images.

6. Complaints

Any complaints about the Parish Council CCTV system should be addressed to the Clerk of the Council.

Complaints will be investigated in accordance with the existing Parish Council complaints procedure.