Gnosall Parish Council
(Including the Wards of Moreton and Knightley).

CCTV Policy

Written:	**July 2020.**
Formally Adopted by Council:	**July 2020.**
Reviewed and Revised:	**June 2023.**
Next Review:	**July 2026.**

Contents.

1. Introduction.

1.1 This policy relates to the management, operation, use and confidentiality of the CCTV system owned and used by Gnosall Parish Council (GPC), The Grosvenor Centre, High Street, Gnosall, ST20 0EX.

1.2 The Chief Officer is responsible for ensuring compliance with this policy.

1.3 Councillors and staff nominated as 'Operators' will be responsible for the operation of the system and retrieval of data.

1.4 This policy MUST be complied with at all times.

2. Data Protection.

3.1 CCTV digital images, if they show a recognisable person, are Personal Data. Consequently, this Policy is associated with the Parish Council's Data Privacy & Protection Policy, the provisions of which should be adhered to at all times.

3.2 The CO is the Parish Council's Data Protection Officer and is responsible for the Council's Data Protection Policy. The Council has adopted the 12 guiding principles of the CCTV code of practice issued by the Information Commissioner's Office, as at Appendix 1.

3.3 The CCTV System is registered with the Information Commissioner and complies with the requirements of the Data Protection Act 2018 (DPA 2018), the General Data Protection Regulation (GDPR) and the Commissioner's Codes of Practice for both CCTV and Data Sharing.

3. The System.

3.1 The system comprises of eight external cameras, two internal cameras and a sixteen-channel digital recorder located at the Gnosall Parish Council office, The Grosvenor Centre, High Street, Gnosall.

3.2 The system records images from the cameras onto a hard drive. Images are stored on the hard drive for a maximum of twenty-eight days, after which recordings are written over.

3.3 Warning signs are prominently placed to inform members of the public that a CCTV installation is in use.

3.4 Although every effort has been made to ensure maximum effectiveness of the system, it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

3.5 The CCTV system is not controlled and monitoring of the cameras is not routinely conducted.

4. Purpose of the System.

4.1 The system has been installed by Gnosall Parish Council with the primary purpose of reducing the threat of crime and anti-social behaviour generally and protecting the Council's premises.

These purposes will be achieved by recording footage from the system cameras to:

- Deter those having criminal intent.
- Assist in the prevention and detection of crime.
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.
- Facilitate the identification of any activities or event which might warrant legal action.

The system will NOT be used:

- to provide recorded images for any form of entertainment.
- to undertake any covert recording.

5. Security of the Information Gathered.

5.1 Images captured by the system will only be viewed if an incident has been reported, although live monitoring will be undertaken by operators as and when necessary.

5.2 No unauthorised access to the data will be permitted at any time. Access will be strictly limited to nominated persons and law enforcement officers.

5.3 The digital recorder will remain securely stored within the Council's office.

6. Recordings.

6.1 Once the hard drive has reached the end of its use it will be erased, prior to disposal.

6.2 All hard drives and recorders shall remain the property of the Council until disposal and destruction.

6.3 Cameras are not and will not be deliberately directed toward private homes, gardens or other areas of private property to record personal and private activity therein.

6.4 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

6.5 Recordings will not be released to the media by Gnosall Parish Council. However, the Council supports the distribution of recordings to the media for use in the investigation of crime, by the police or other law enforcement agency, when it is necessary to do so.

7. Disclosure of Recorded Material.

7.1 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder.
- Prosecution agencies.
- Relevant legal representatives.
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

8. Access by the Data Subject.

8.1 GPC acknowledges that Data Subjects (individuals to whom 'personal data' relate) have a right to data held about themselves, including those obtained by CCTV. They do not, however, have the right of instant access.

8.2 Requests for Data Subject Access should be made to the Chief Officer (CO).

8.3 The CO will then arrange for a copy of the data to be made and given to the applicant on media supplied by the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the CO. A response will be provided promptly and in any event within forty days of receiving the information.

8.4 The Data Protection Act gives the CO, as the Data Protection Officer, the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

8.5 An individual has the right to request a prevention of processing where this is likely to cause substantial and unwarranted damage or distress to that or another individual.

8.6 All such requests should be addressed in the first instance to the CO as the Data Protection Officer, who will provide a written response within 21 days of receiving the request setting out their decision. A copy of the request and response will be retained.

9. Download Procedures.

9.1 A separate copy of downloaded images will only be retained, when necessary, for GPC purposes, such as in the pursuit of a civil claim by GPC or, in the case of ongoing issues, where a file of evidence is being compiled.

9.2 A separate copy of downloaded images will **not** be retained when they are requested by and provided to other agencies, e.g., the Police.

9.3 In order to maintain and preserve the integrity of the media used to store recordings from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

9.3.1 A record will be maintained of the release of data to authorised applicants, by an operator.

9.3.2 Any storage media must be provided by the authorised applicants requesting the data and cleaned of any previous recording. Storage media WILL NOT be provided for evidential purposes.

9.3.3 An operator shall record the date and time of the recorded footage, the date and time of the transfer of the footage onto separate media the details of the person to who the recording was provided.

9.3.4 Any media required for evidential purposes must be sealed in a provided evidential bag that is signed and dated by the operator providing the data.

10. Breaches of Policy (including Breaches of Security).

10.1 Any breach of this policy by Councillors or Council Staff, will be initially investigated by the CO, in order for them to take the appropriate action.

10.2 Any breach may be referred to the Information Commissioner's Office.

11. Complaints.

11.1 Any complaints about the Parish Council's CCTV system should be addressed to the CO.

12. Compliance Monitoring.

12.1 The contact point for members of the public wishing to enquire about the system will be the Clerk by telephone on (01785) 822 685, email clerk@gnosallparishcouncil.org.uk, or by attending the Parish Office during opening hours.

12.2 Upon request enquirers will be provided with:

- A copy of this policy.
- An access request form, if required or requested.
- A subject access request form, if required or requested.
- A copy of the Council's complaints procedures.

12.3 All documented procedures will be kept under review and a report periodically made to the Grosvenor Centre Committee.

12.4 The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Grosvenor Centre Committee.

Appendix 1: The Guiding Principles of the Surveillance Camera Code of Practice.

Gnosall Parish Council has adopted the following 12 guiding principles:

1. 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.

2. 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.

3. 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.

4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

5. 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.

6. 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 its purpose has been discharged.

7. 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.

8. 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.

9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

10. 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.

11. When the use of a surveillance camera system is in pursuit of a legitimate aim and a pressing need, 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.

12. Any information used to support a surveillance camera system which matches against a reference database for matching purposes should be accurate and kept up to date.