

Norton Parish Council

CCTV Policy

1 Introduction

1.1 This policy is to control the management, operation, use and confidentiality of the CCTV system sited on Norton Village Hall covering the car park, playing field and play area, Ixworth Road, Norton.

1.2 It has been prepared taking due account of the Code of Practice published by the Data Protection Commissioner (July 2000).

1.3 This policy will be subject to periodic review by the Parish Council to ensure that it continues to reflect the public interest and that the system meets legislative requirements.

1.4 The system comprises of 5 fixed cameras.

2. Objectives of the scheme

- (a) To protect the building and its assets
- (b) To increase personal safety and reduce the fear of crime
- (c) To support the Police in a bid to deter and detect crime
- (d) To assist in identifying, apprehending and prosecuting offenders
- (e) To protect members of the public and private property
- (f) To assist in managing the playing field and play area.

3. Statement of intent

3.1 The CCTV Scheme will be registered with the Information Commissioner under the terms of the General Data Protection Act of May 2018 and will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

3.2 The Parish Council will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act.

3.3 Cameras will be used to monitor activities within the Recreation Ground and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the Recreation Ground, together with its visitors.

3.4. The cameras are not to focus on private homes, gardens and other areas of private property.

3.5 Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the Parish Councils forms for Directed Surveillance to take place, as set out in the Regulation of Investigatory Power Act 2000.

3.6 Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.

3.7 The planning and design has endeavoured to ensure that the Scheme will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

3.8 Warning signs, as required by the Code of Practice of the Information Commissioner have been placed at all access routes to areas covered by the CCTV.

4 Operation of the system

4.1 The Scheme will be administered and managed by the CCTV control group consisting of the Parish Council Chairman and Vice Chairman and appointed representative of the Village Hall Management Committee in accordance with the principles and objectives expressed in the code.

4.2 The day-to-day management will be the responsibility of the CCTV control group

4.3 The CCTV system will be operated 24 hours each day, every day of the year.

5. Control Room

5.1 The CCTV control group will routinely check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.

5.2 Access to the CCTV Control Room will be strictly limited to the CCTV control group

5.3 Unless an immediate response to events is required, the CCTV control group must not direct cameras at an individual or a specific group of individuals.

5.4 Visitors and other contractors wishing to enter the Control Room will be subject to particular arrangement as outlined below.

5.5 If out of hours emergency maintenance arises, the CCTV control group must be satisfied of the identity and purpose of contractors before allowing entry.

5.6 A visitor's book will be maintained in the Control Room. Full details of visitors including time/date of entry and exit will be recorded.

5.7 Other administrative functions will include maintaining hard disc space, maintaining occurrence and system maintenance logs.

5.8 Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. Liaison

6.1 Liaison meetings (4 times a year) may be held with all bodies involved in the support of the system.

7. Monitoring procedures

7.1 Camera surveillance may be maintained at all times.

7.2. A monitor is installed in the Control Room to which pictures will be continuously recorded.

7.3 If covert surveillance is planned or has taken place copies of the Authorisation Forms, including any Review, or Cancellation must be returned to the Parish Clerk.

7.4 The CCTV is viewable from the machine installed in a secure cupboard in the village hall by a member of the control group only.

7.5 CCTV data is viewable remotely via log in details and password protected internet access restricted to the Parish Council Chairman only.

8. Recording procedures

8.1 In order to maintain and preserve the integrity of the data the following procedures for use and retention must be strictly adhered to:

- (i) Data stored on the hard drive may be copied to a usb device if required for evidence purposes by a member of the Control Group only.
- (ii) Data stored on hard drive will be stored for 30 days with an auto re-write regime in place.
- (iii) Data required for evidential purposes and copied to a usb device, must be witnessed, signed by the controller, dated and stored in a separate, secure, store.

8.2 Data may be viewed by the Police for the prevention and detection of crime, authorised officers of Norton Parish Council (Chair and Vice Chair) for supervisory purposes, authorised demonstration and training.

8.3 A record will be maintained by the Control Group of the release of Data to the Police or other authorised applicants.

8.4 Viewing of Data by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under section 29 of the Data Protection Act 1998.

8.5 Should data be required as evidence, a copy may be released to the Police under the procedures described in paragraph 8.1 (iv) of this Code. Data will only be released to the Police on the clear understanding that the data remains the property of the Parish Council, and both the data and information contained on it are to be treated in accordance with this code. The Parish Council also retains the right to refuse permission for the Police to pass to any other person the data or any part of the information contained thereon. On occasions when a Court requires the release of an original data this will be produced from the secure evidence store, in its sealed bag.

8.6 The Police may require the Parish Council to retain the data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the Police.

8.7 Applications received from outside bodies (e.g. solicitors) to view data will be referred to the Parish Clerk. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. A fee can be charged in such circumstances: £10 for subject access requests; a sum not exceeding the cost of materials in other cases.

9 Breaches of the code (including breaches of security)

9.1 Any breach of the Code of Practice by Council staff, will be initially investigated by the Parish Clerk, in order for him/her to take the appropriate disciplinary action.

9.2 Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10 Assessment of the scheme and code of practice

10.1 Performance monitoring, including random operating checks, may be carried out.

11 Complaints

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

11.2 Complaints will be investigated in accordance with Section 9 of this Code.

12 Access by the Data Subject

12.1 The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

12.2 Requests for Data Subject Access should be made on an application form available from the Parish Clerk. The forms will also be available to the public.

13 Public information

Copies of this Code of Practice will be available to the public from the Parish Clerk.

Summary of Key Points

- This Code of Practice will be reviewed every two years.
- The CCTV system is owned and operated by the Parish Council.
- The Control room will not be manned.
- Liaison meetings may be held with the Police and other bodies.
- Data may only be viewed by Authorised Parish Council Officers and the Police.
- Data required as evidence will be properly recorded and witnessed before being released to the police.
- Data will not be made available to the media for commercial or entertainment.
- Data will be auto-erased after 30 days.
- Any Covert Surveillance or use of a Covert Human Intelligence Source being considered or planned as part of an operation must comply with the corporate policies and procedures. The Parish Council must use these procedures and comply with the requirements set out in the procedure documentation.
- Any breaches of this code will be investigated by the Parish Clerk. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Parish Council.

This CCTV Policy was compiled on 5th August 2019

Adopted by Parish Council on 5th August 2019

THIS POLICY MUST BE COMPLIED WITH AT ALL TIMES.

I have read the above policy and agree to abide by these instructions. I will discuss any concerns with the Clerk to the Council at any time.

Signed Print Name

Date/...../.....

(Operators are issued with their own copy of this policy and shall sign to confirm receipt and compliance.)