CCTV POLICY

Introduction

This Policy is to control the management, operation, use and confidentiality of the CCTV system at the Community Office. It was prepared in 2017 after taking due account of the Code of Practice published by the Data Protection Commissioner (July 2000). 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.

Whitwick Parish Council accepts the principles of the 1998 Act based on the Data Protection Principles as follows:

- data must be fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive'
- accurate;
- not kept for longer than is necessary;
- processed in accordance with individuals' rights;
- secure;
- not transferred to countries with adequate protection;
- subject to guidance on good practice;
- examples of how to implement the standards and good practice.

Background

After discussion at several Council meetings (agendas and minutes of which are available to the public) a new scheme was installed in 2016 for prevention of crime and protection of staff. After consultation with the police and specialists, this was designed to monitor visitors via the front entrance to the Community Office and to give external monitoring of the front/side and internal areas of the building, plus digital recording via a standalone hard drive system. Due to public use of council facilities, recording is carried out 24 hours per day, 365 days of the year. Surveillance of colour monitors is undertaken by staff who, whilst not specifically employed for CCTV monitoring, are undertaking other duties but who already have an overall remit for safety of public visitors and protection of council property and premises.

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 using Council facilities so they can enter and leave the building 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 byelaws;
- to deter potential offenders by publicly displaying the existence of CCTV, having cameras clearly sited that are not hidden and signs on display, both inside and outside the Community Office.
- to assist all "emergency services" to carry out their lawful duties.

Changes to the Purpose or Policy
A major change that would have a significant impact on either the purpose or this policy of operation of the CCTV scheme will take place only after discussion at Council Committee meeting(s) and resolution at full Council meeting. All agendas are posted on the Parish Council notice board at least 3 clear days before Council meetings.

Responsibilities of the Owners of the Scheme
The elected Parish Council retains overall responsibility for the scheme.

Management of the System
Day-to-day operational responsibility rests with the Parish Manager, who can be consulted by staff out of hours, if and when necessary.

Breaches of this policy by operators will be investigated by the Parish Manager and reported to the Property Management and General Purposes Committee.

A CCTV system prevents crime largely by increasing the risk of detection and prosecution of an offender. Any relevant images or digital evidence must be in an acceptable format for use at Court hearings. This policy must be read and understood by all persons involved in this scheme and individual copies of this policy will therefore be issued for retention. A copy will also be available for reference in the secure recording area(s).

Control and Operation of the Cameras, Monitors and Systems.
The following points must be understood and strictly observed by operators:

1. Trained operators must act with due probity and not abuse the equipment or change the pre-set criteria to compromise the privacy of an individual.
2. The position of cameras and monitors have been agreed following consultation with the police and security consultants in order to comply with the needs of the public.
3. No public access will be allowed to the monitors except for lawful, proper and sufficient reason, with prior approval of the Parish Manager or by application to the Council/Committee. The Police are permitted access to images and data if they have reason to believe that such access is necessary to investigate, detect or prevent crime. The Police are able to visit the Community Office to review and confirm the Parish Council's operation of CCTV arrangements. Any visit by the Police to view images will be logged by the operator.
4. Operators should regularly check the accuracy of the date/time displayed.
5. Digital records should be securely stored to comply with data protection and should only be handled by the essentially minimum number of persons. Digital images are retained for a maximum of 15 days and erased automatically according to the system settings.
6. Images will not normally be supplied to the media, except on the advice of the police if it is deemed to be in the public interest. The Parish Manager would inform the Chairman of the Council and/or Property Management and General Purposes Committee of any such emergency.
7. As records may be required as evidence at Court, each person handling a digital record may be required to make a statement to a police officer and sign an exhibit label. Any images that are handed to a police officer should be signed for by the police officer and information logged to identify the recording, and showing the officer's name and police station. The log should

also show when such information is/if returned to the Parish Council by the police and the outcome of its use.

8. Any event that requires checking of recorded data should be clearly detailed in the log book of incidents, including Crime Nos. if appropriate, and the Council notified at the next available opportunity.
9. Any damage to equipment or malfunction discovered by an operator should be reported immediately to their line manager or contact made with the company responsible for maintenance, and the call logged showing the outcome. When a repair has been made this should also be logged showing the date and time of completion.
10. Any request by an individual member of the public for access to their own recorded image must be made on an 'Access Request Form' and is subject to a standard fee. Forms are available from the Community Office and will be submitted to the next meeting of the appropriate Council/Committee for consideration and reply, normally within 40 days.

Accountability

Copies of the CCTV Policy are available in accordance with the Freedom of Information Act, as will any reports that are submitted to the Parish Council *providing it does not breach security needs.*

The Police will be informed of the installation and provided with a copy of this CCTV Policy.

Any written concerns, complaints or compliments regarding the use of the system will be considered by the Parish Council, in line with the existing complaints policy.

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 Parish Manager 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.)

INFORMATION TECHNOLOGY POLICY

Staff are other users are asked to read and comply with the following guidelines when using computers, technology and Internet connections provided by this Council.

1. The Parish Council provides access to computers, phones, scanners, copiers and the Internet for staff as it is deemed to be an important source of public information which can help contribute to the work of this Council and be helpful to residents of Whitwick.
2. The Parish Council encourages electronic communications with local, national and international organisations.
3. The Parish Council cannot control and is not responsible for the accuracy or content of information gathered over the Internet. However, filtration software is used in an effort to protect users from unsuitable sites.
4. **However it remains the role of staff to avoid deliberate use of the Council's Internet connections and technology for inappropriate personal use. Staff should immediately alert the Parish Manager of any suspect material found stored on any computer or elsewhere on the premises.**
5. Staff and users are expected to use technology in a courteous, reasonable and responsible manner. The following activities are not acceptable and anyone found to be involved in them may face disciplinary action or other consequences:
    - Receiving, sending, or displaying offensive messages or pictures
    - Using obscene language
    - Improper use of e-mail and faxes
    - Damaging computers, computer systems or computer networks
    - Violating copyright laws
    - Using passwords and identities belonging to other people
    - Trespassing in folders, works, or files belonging to other people
    - Intentionally wasting limited resources
    - Employing the network for commercial purposes
    - Employing the network for illegal activities
    - Downloading any commercial software
6. The Internet and computer equipment and software must be used as installed. Staff and users may not add, delete or change anything on Council computers. Any system requests to download add-ins should be referred to the Parish Manager.
7. The Parish Council uses a virus-checker on the computers. Staff and users are reminded that external devices are a potential high risk and must make every endeavour to completely protect the systems from getting a computer virus. If an infected device is loaded onto any other computer, it could cause damage to that computer, and consequently to other network use.
8. Access to chat rooms and gaming are not permitted on Council computers.

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 Parish Manager at any time.

Signed …… Print Name …… Date ……../……/…….

(Staff are issued with two copies of this policy, one to retain and one to sign and return to the Parish Manager).