

# Driffield Town Council

## CCTV Code of Practice

## Contents:

1. Introduction .....	3
2. Location.....	3
3. Signage .....	3
4. Purpose Of The System .....	4
5. Management.....	4
6. Responsibilities of Processors.....	5
7. Control Centre, Monitoring Arrangements and Access to the System .....	5
8. Access to and Security of Monitoring .....	5
9. Legislative framework.....	6
10. Regulations of Investigatory Powers Act (2000) (RIPA).....	6
11. Right of Access .....	6
12. Camera Siting, Image Quality and Access .....	8
13. Consultation.....	11
14. Complaints Procedure .....	11
15. Disciplinary Action .....	11
16. Changes to This Code of Practice.....	11

## 1. Introduction

This CCTV Code of Practice details the use of CCTV by Driffield Town Council including the protection of law abiding citizens. It also provides guidance on producing evidence against perpetrators of criminal action.

It introduces measures to ensure accountability, high standards, good quality information and effective partnerships between the Police and the System owners.

The purpose of this document is to state the intention of the CCTV owners and the CCTV system operators on behalf of the Driffield Town Council ('the Council') and outline how it is intended to be operated. It has been drawn up to govern the management of the CCTV Surveillance system.

Due to the constant changes in legislation this Code of Practice will be reviewed and amended as appropriate after any changes are made to the system, or on an annual basis, by the CCTV committee. It will be available to the public at Driffield Town Council offices and on the Council's website. Amendments will be recorded and published.

All recorded material is the property of Driffield Town Council and is subject to the statutory requirements of the General Data Protection Regulation (2016), Data Protection Act 2018, the Freedom of Information Act 2000, the Human Rights Act (1998), the Regulation of Investigatory Powers Act 2000 and in accordance with this Code of Practice.

The CCTV System will only be used to achieve purposes set out in this Code of Practice. Cameras will at no time overlook or be used to look into private residences/premises without receiving prior consent from the occupiers of those premises. No sound recording will be used in public places. There will be no interest shown in, or deliberate monitoring of, people going about their legitimate business.

## 2. Location

This Code of Practice relates to the Closed Circuit Television System (CCTV) installed in the town of Driffield as defined by the Data Protection Impact Assessment (DPIA) for the system.

The control centre is located at Driffield Police Station. The control centre is operated and managed by employees of Humberside Police as processors on behalf of the Council in the event of a subject access request or in response to incidents relating to purposes of law enforcement. At this point as a competent authority Humberside Police become the controllers of that data. Driffield Town Council are not a competent authority for the purposes of law enforcement.

## 3. Signage

All CCTV systems shall have appropriate signage in accordance with the General Data Protection Regulation, advising people that CCTV is in operation.

These signs need to be placed on the perimeter of the CCTV system and other strategic places.

The CCTV signs will vary in size according to location and the circumstances.

Each sign shall contain the identity of the organisation responsible for the scheme and its purpose. The name and contact number of the controller should be given for further information about the scheme.

If signs are to be installed on public highways, then permission and advice on siting must be sought from the East Riding of Yorkshire Council.

## 4. Purpose Of The System

This Code of Practice sets out to ensure the most effective use of the CCTV system to prevent crime and disorder. It endeavours to uphold the safety and civil liberties of those who live, work and visit the town.

CCTV, where it is considered beneficial, should always be used as part of a wider crime prevention strategy, not as a sole means.

CCTV plays an important part in our fight against crime but it should be used wisely and follow this Code of Practice.

### **The purpose and use of the system is to achieve the following aims:**

- a) Providing the Police and the Council with evidence to take criminal and civil action in the Courts.
- b) Reducing the fear of crime and providing reassurance to the public.
- c) Providing assistance in the prevention of crime.
- d) Assisting with the maintenance of public order.
- e) Deterring or reducing the incidence of vandalism, graffiti, and other environmental crime.
- f) Deterring persons from committing crimes and to enhance the opportunities for identifying those who do.
- g) Improving the safety and security of residents, visitors and the business community.
- h) Discouraging anti-social behaviour including alcohol and drug-related elements.
- i) Assisting aspects of Town Centre Management.

The Council is committed to maintaining, reviewing, and enhancing the systems and this code of practice in order to improve their effectiveness. It is also committed to maintaining civil liberties.

## 5. Management

The CCTV system is operated in partnership with Humberside Police although the Council retains overall control as follows:-

**The owner of the system is:-** Driffield Town Council of 1-4 Market Walk, Driffield, East Yorkshire, YO25 6BW.

**The controller is:** Driffield Town Council

**The Processor is :-** Humberside Police, Police Headquarters, Priory Rd, Hull HU5 5SF

**Enquiries:** Town Clerk. Driffield Town Council, 1-4 Market Walk, Driffield, East Yorkshire, YO25 6BW.

Telephone: **01377 254160**      Email: [townclerk@driffieldtowncouncil.gov.uk](mailto:townclerk@driffieldtowncouncil.gov.uk)

## 6. Responsibilities of Processors

Processors using the system have responsibility for:

1. Respond to requests for information in accordance with the Data Protection Act 2018
2. The protection of the interests of the public and of the individual as far as is practical.
3. Compliance with this Code of Practice.
4. Compliance with CCTV Operational Manual.
5. Compliance with all legislation pertaining to the use of the system.

## 7. Control Centre, Monitoring Arrangements and Access to the System.

Control Centre. The control centre is located at Driffield Police Station. This is for reasons of practicality (given the purposes of the system) and the security of the system. It is operated and managed by employees of Humberside Police under agreement from the Council. The Police have been designated as Processors on behalf of the controller and have operational access to view any of the Council's CCTV installations for law enforcement purposes and responding to requests for information made by a data subject.

## 8. Access to and Security of Monitoring

CCTV data is recorded 24 hours a day, 365 days a year but images are not continuously or actively monitored. The processor has controlled access to the control room 24 hours a day. Images are only accessed by processors in the following circumstances: -

- In response to specific incidents in order to protect the interests of the public and the individual as far as is practical.
- or the detection, prevention and prosecution of crime.
- At the request of the controller in response to Subject Access Requests.
- At the request of the controller in response to legitimate requests from authorised third parties.

Access to the control room is strictly controlled. Access to view the monitors, whether to operate the equipment or to view the images, is limited to authorised staff who have been designated and are trained in that responsibility.

Only authorised personnel are to be admitted to the control room. The names and photographs of all authorised personnel are to be held within the control room and all such staff must carry an official identification card.

The control room must not be accessed by unauthorised personnel and access to monitors and recordings is not allowed except for compliance under subject access or law enforcement purposes.

All staff who have access to the monitors are fully trained in legislation issues, monitoring, handling, disclosure, storage and deletion of information, disciplinary procedures, incident procedures, limits on system uses.

## 9. Legislative framework

**General Data Protection Regulation (2016), CCTV Code of Practice (2014) and The Human Rights Act (1998).**

The Council has an obligation to comply with the requirements of the General Data Protection Regulation (2016). All CCTV Systems which record images (data) must be registered under the General Data Protection Regulation and as such the CCTV system is registered with the Information Commissioners Office. Driffield Town Council's Registration number is Z2777491.

The Council recognises that the use of CCTV could potentially impact upon a member of the public's right to respect for private and family life as accorded in article 8 of the Human rights Act (1998). CCTV will therefore only be used for the prevention and detection of crime or disorder, to ensure and/or maintain public safety within the Driffield Town Area.

## 10. Regulations of Investigatory Powers Act (2000) (RIPA)

Driffield Town Council and its partners **do not** engage in covert, directed or intrusive surveillance. If this became necessary, the appropriate authority would be obtained from the relevant authority. In this instance surveillance would only be carried out for the duration required for the intended purpose.

## 11. Right of Access

### a. Subject Access Request

Under The General Data Protection Regulation an individual is entitled to be informed of the following detail:-

- Confirmation that their data is being processed, and
- To a copy of their personal data

Subject Access Requests can be made in written or verbal form and sent to the Controller. Subject Access Request forms are available on the Council website at the following link - [Subject Access Form](#).

The information must be provided without delay and at the latest within one calendar month of the request being made. The Controller must also provide the information which forms the personal data, i.e., a copy of the recordings. A copy must be provided free of charge however a 'reasonable fee' may be charged if the request is manifestly unfounded or excessive.

Identifiable images (personal data) of other persons (data subjects) in video footage are pixelated so that these individuals cannot be identified. Identifiable images of other persons in static images are redacted so that these individuals cannot be identified. Any other identifiable information such as vehicle registration marks or vehicle sign writing will also be redacted.

## b. Appeals and Complaints

Complaints and queries should be directed in the first instance to Driffield Town Council who will then refer them to Humberside Police (the processors) and their data protection officer who will initiate a review. All complaints and subsequent findings and outcomes will be communicated to the CCTV Committee Meetings to ensure a clear reporting and documentation system and that DTC retains and can clearly demonstrate oversight of the process and influence the rigorousness of any investigation undertaken. If an individual believes that a Controller has failed to comply with a subject access request in contravention of GDPR, they may ask for an internal review which will be carried out by the processors data protection officer or they can complain directly to the Information Commissioners Office at Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

## c. Freedom of Information Requests

Freedom of Information requests must be made to the Driffield Town Council. The Information must be provided without delay and at the latest within 20 days of receipt of the request.

However, the GDPR can override the FOIA where this would infringe the rights of data subjects in CCTV images. Therefore any request for CCTV footage/images made under the FIOA must take account of the GDPR.

## d. Access to and Disclosure of Images

All requests for the disclosure of data will be processed and should be made to the Controller. No CCTV images will be sold (or given) for another purpose.

## e. Requests to view Data

Requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:

- Providing evidence in criminal investigations or proceedings (Police and Criminal Evidence Act (1984), Criminal procedure and Investigation Act (1996).
- Providing evidence in civil proceedings.
- Prevention of crime and disorder.
- The investigation and detection of crime (this may include the identification of offenders).
- Identification of witnesses.
- Public Interest.
- Third parties, which are required to show adequate grounds for the disclosure of data within the above criteria, may include but are not limited to:
  - Law Enforcement Agencies.
  - Statutory Authorities with powers to prosecute (E.g., Customs and Excise, Trading Standards, etc)
  - Solicitors acting on behalf of the data subject by consent or another authority.
  - Plaintiffs in civil proceedings.

The Controller of Driffield Town Council has responsibility for the management of data within Driffield Council. However, once the data has been downloaded by the processor and handed over to a third party, the responsibility for making decisions about and protecting that data becomes the responsibility of the Controller receiving that data.

Any members of the general public who approach the Council requesting to view the content of any CCTV images regarding any incident will also be advised to report the matter to the Police for further investigation.

#### f. Media Disclosure

CCTV images will not be given to the media for broadcast or reproduction. Images disclosed to the media in the public interest, because public assistance is required to identify a perpetrator or a victim of crime and/or to assist in solving a crime, should only be disclosed by the Police.

## 12. Camera Siting, Image Quality and Access

### Overview of the system

A complete Data Protection Impact Assessment (DPIA) of the whole system and each CCTV camera in use and this Code of Practice will be updated on completion of this assessment.

The DPIA will document Driffield Town Council's CCTV system including, but not limited to:-

- a) Any measures that have been taken to minimise intrusion of privacy
- b) Regular planned maintenance to ensure the functionality and integrity of the CCTV system takes place on a monthly basis.

### Consideration Before Purchase of CCTV Systems and Equipment.

In considering the installation of a CCTV systems and equipment, the Council will ensure that it complies with GDPR and this Code of Practice and in so doing, prior to purchase, satisfy its requirements on:

- The justification for the system and equipment including assessment of its impact on people's privacy by undertaking a Data Protection Impact Assessment (DPIA).
- The purpose of the CCTV system with evidence to suggest its introduction will satisfy the demand.
- The CCTV systems purpose linked with other crime prevention measures.
- The adequacy of the procedures for System Management.
- Planned maintenance required by the system.

### Image Quality

In the likely event that CCTV recorded images are to be used as Court evidence, the following questions should be considered:

- a) What level of detail are the cameras expected to identify, e.g. groups of people, individuals, vehicle registration marks etc?
- b) What operational requirements are needed, i.e., night-time efficiency (there are 4000 hours of darkness per annum).
- c) Number of cameras.
- d) Colour or monochrome.



- e) The frequency of time-lapse recording e.t.c.
- f) Consider measures to protect the CCTV cameras from vandalism.
- g) Cost - Can the subsequent revenue costs for running the system be afforded?

### Further Information

Useful information can be obtained by browsing the Home Office web site <http://www.homeoffice.gov.uk> and the Information Commissioners Office web site <http://www.ico.gov.uk>

The Home Office has provided a number of informative documents some of which are as follows;

- CCTV – Looking Out for You
- CCTV Operational Requirements Manual
- National CCTV Strategy

There are other useful sources of information;

- The British Security Industry Association has published a "User Guide to CCTV Systems Performance"
- The Local Government Association
- The Home Office Scientific Development Branch
- Surveillance Camera Commissioner Code of Practice

### Digital Image Recording Procedures (Data Processing)

GDPR requires that appropriate steps are taken to avoid unauthorised or unlawful data processing. Apart from data subjects, access to recorded images is therefore limited.

Data processors complete a register on every occasion that CCTV data is processed (i.e., viewed or downloaded).

Adhering to the agreed management and operational procedures is crucial if the digital recordings produced are to be of sufficient evidential value and quality that they can be used for intelligence gathering purposes or as evidence to be produced in a court.

Digital images are automatically recorded and are kept for 31 days on the hard drive of the recording equipment, after which the images will be overwritten.

For evidential purposes each recorded image downloaded should have the correct time and date automatically embossed on it, therefore it is essential that operators periodically check that images recorded are correct.

If a request for access to recorded images is made within the 31 days, then only copies of the images that have been specifically requested can be downloaded.

These images can be downloaded on either DVD or CD-ROM formats which should be clearly labelled as private and confidential.

## Digital Recording Viewing/Copying Procedure (Data Processing)

On receiving a request to view a digital recording of a particular incident, the following process should be followed:

- To preserve the continuity of evidence a record should be created for a copy made of any digital recording (CCTV Access Register).
- Each digital image recording released should be clearly identified with the relevant incident report number, start and finish time, date of the incident and the Police incident number.
- No images should be released either wholly or partially to any other third party without written consent from Driffield Town Council in accordance with a Data Subject Access Request.
- Once released into Police possession the data is no longer the responsibility of Driffield Town Council and becomes the responsibility of the Humberside Police Controller
- A record of all data released will be kept by the Police and a copy given to the Driffield Town Council Data Controller on a monthly basis to facilitate Data Controller oversight.

The report should include the following:

- The name, rank and title of the person requesting the viewing or copy.
- The organisation that person represents and the incident type.
- Date, time and location of incident.
- Police/Fire Service Force Wide Incident Number (FWIN) if applicable.
- The name of the Humberside Police Controller.

## Local Recording

A CCTV system, which is recorded on site (i.e. there is no connection to the main system) is known as a Locally Recorded System.

There a number of locally recorded facilities in use and these supplement the central recording system. The location of locally recorded systems is not public knowledge in order to protect their safety and security. As technology advances, this situation may change and therefore the Council will keep CCTV development under constant review.

## Recording Equipment and Data Security

All CCTV equipment at central and locally recorded sites is securely stored to prevent theft, loss etc and each system is encrypted and password protected to maintain the security and integrity of the data.

**In the unlikely event that recording equipment is stolen, or data is lost or breached either deliberately or accidentally this must be reported to the ICO as the earliest opportunity and at the latest within 72 hours of the Council becoming aware of this.**

## Data Retention and Disposal

All CCTV images recorded shall be kept for 31 days after which they will be automatically overwritten unless an access request has been made by:-

- a data subject,

- the Police for the purpose of any criminal investigation. Or for,
- Any legal obligation for access under Data Protection Legislation.

### 13. Consultation

Driffield Town Council works in partnership and prides itself on its participation, co-operation and communication with all interested parties in the fight to prevent and reduce crime.

The salient points of the consultation strategy are:

- Any proposed CCTV system must be the subject of adequate research and consultation within the area to be covered by the camera system and where applicable the adjacent areas and include a Data Protection Impact Assessment. (DPIA)
- No CCTV system will be considered unless it has the Council and Divisional Police Chief Superintendent's support.
- A CCTV System must not infringe legislation on human rights issues, for example, privacy and this must be explained as part of any consultation process.
- All parties involved in consultation must be informed about the provisions relating to CCTV contained in the General Data Protection Regulation (2018) and the CCTV Code of Practice 2014.

### 14. Complaints Procedure

Any complaints regarding the use of CCTV should be directed to the Town Clerk as per the Council's Complaints Procedure. The Complaints Procedure can be found on our website. Any complaints received against the Police must be forwarded immediately to the Divisional Chief Superintendent based Humberside Police Headquarters, to be dealt with through normal Police procedures.

### 15. Disciplinary Action

The appropriate disciplinary action should be implemented where there is a deliberate breach of security procedures (or this Code of Practice) and staff should be made aware of such disciplinary procedures.

### 16. Changes to This Code of Practice

Minor changes to the Codes of Practice and Operational Manual that are required to efficiently maintain the Operational System may be made by the Controller and published on the Council website.

Any major changes to the Code of Practice Operational Manual will be agreed by the Driffield Town Council CCTV Committee and published on the Council website.


Any amendments made should be recorded on the Schedule of Amendments log (Appendix 3).

## **Certificate of Agreement**

The content of this Code of Practice is hereby approved in respect of the Drifffield Closed Circuit Television System and, as far as is reasonably practicable, will be complied with by all who are involved in the management and operation of the System.



Signed for and on behalf of the Driffield Town Council

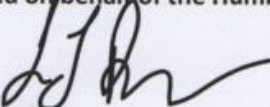
Signature: 

Name: CLR PAUL ROUNDING

Position Held: CHAIRMAN CCTV COMMITTEE

Dated: 28/7/2020

Signed for and on behalf of the Humberside Police

Signature: 

Name: Ewan Robson

Position Held: information Compliance Unit Manager/ Data Protection Officer

Dated: 28/07/2020

# APPENDIX 1

## Definitions/Glossary of Terms

In relation to GDPR and the CCTV Code of Conduct the following terms have the following meanings.

**Controller:** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

**CCTV:** means cameras, devices or systems including fixed CCTV and any other systems that capture information of identifiable individuals or information relating to identifiable individuals.

**Personal Data:** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**Data Subject:** means any individual who can be identified directly or indirectly from CCTV Data (or any other Data in an organisations possession).

**Controller:** is the organization (or persons within it) which determines how and for what purpose the personal data are processed.

**CCTV Processors:** are employees of an organisation (or employees of any Processors appointed by an organisation) whose work involves processing CCTV Data. This includes those whose duties are to operate CCTV to record, monitor, store, retrieve and delete images. Processors must protect the CCTV Data they handle in accordance with Data Protection legislation and local Data Protection policies and procedures.

**Processing:** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

**Processor;** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

