CCTV Code of Practice

Wem
CCTV Scheme

Introduction

This Code of Practice sets out the means by which Wem Town Council operates its CCTV. It is a public document and may be made available to any interested party. There is a legal requirement for Wem Town Council to manage the systems properly and in compliance with current legislation. Wem Town Council should be considered as a public authority for the purposes of the Human Rights Act 1998.

The Surveillance Camera Commissioner Code of Practice is considered a statutory instrument.

This code relates to overt, public CCTV cameras, intrusive covert use of cameras within this CCTV scheme is dealt with under operating procedures and governed by legislation outlined in this code.

Background

Surveillance camera systems are deployed extensively within England and Wales, and these systems form part of a complex landscape of ownership and operation. Where used appropriately, these systems are valuable tools which contribute to public safety and security and in protecting both people and property
This has brought about the need to have a universal code or practice to ensure effective and ethical use of CCTV in the public sector.
.

The Data Protection Act 2018 requires images (personal data) to be carefully and lawfully handled. It gives the public at large a right to prevent CCTV causing them personal distress or damage and allows for damages to be awarded when breached, as well as giving them certain rights of access to those images.

In October 2000, the Human Rights Act placed the operating of CCTV by public authorities on a legal footing, requiring specific objectives and aims in order to record images from the public at large.

The Protection of Freedom Act 2012 also creates the role of the Surveillance Camera Commissioner, who now has a formal role in the regulation of CCTV operated by relevant public authorities

Liability
Data Controllers, Data processors, Managers and operators of this CCTV scheme and associated equipment will not be held liable for any act that is unrecorded by the system.

1. Section One

Protocol

1.1 Purpose

The purpose of this Code of Practice is to regularise a protocol for the existing good practice, within a common framework for managing and operating existing or planned CCTV schemes in the Wem area. Wem CCTV System is owned by Wem Town Council and should be operated in an open and public way as members of the public will be filmed using the system. It will be considered as ***Public Space Surveillance*** under the terms of the Data Protection Act 2018 and Private Security Industry Act 2001.

1.2 Aims of Wem CCTV System

1.2.1
Wem Town Council surveillance cameras will only be used for the following reasons:

- Prevention and detection of Crime and anti-social behaviour and the apprehension and prosecution of offenders
- Reduce the fear of crime and to reassure the public
- To provide the Police, Local Authority, H.M Customs and Excise, The Health and Safety Executive and other Law Enforcement Agencies with evidence upon which to take criminal and civil action in Court
- Improve and maintain Police Officer and Police Staff safety and assist other 'Emergency Services'

1.3 Intention

1.3.1
The CCTV system used by Wem Town Council record images from public places via a secure recording system in order to achieve the objectives shown in paragraph 1.2.1 above. The use of such a system provides the means by which evidence may be recorded 24 hours if required a day and by which images can be made available for court proceedings or other applications. For the purpose of this code, *a public places means any place to which the public normally have access whether on payment or otherwise*.

1.3.2
In cases where specific monitoring is required, which falls outside of this code, appropriate authority must be obtained in order to comply with legislation.

1.3.4
Wem Town Council must comply with the Human Rights Act 1998 at all times. The following articles will be complied with:

- Article 3: Cameras will not be used where they may cause persons to be subject to inhuman or degrading treatment.
- Article 8: Cameras will not be used (unless authorised in law) where they prevent persons from enjoying respect for their family life
- Article 14: Cameras will not be used in a manner which causes persons to be discriminated against

1.3.5
Under the current system Wem Town Council does not transmit images to any other agency. ,

1.3.6
This code should apply to future schemes and the expansion of the current one.

2. Section Two Code of Practice

2.1 Data Protection Act 2018

2.1.1
Wem Town Council is registered with the Information Commissioner Reference ZA011535

On 25th May 2018 the General Data Protection Regulations (GDPR) came into effect and they set out the requirement for the collection of personal data. Article 4 of GDPR states:

Where personal information is processed, data (images) must be:

a) Processed fairly and lawfully
b) Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
c) Adequate, relevant and not excessive in relation to the purposes for which they are being processed
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate is erased or rectified.
e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unlawful processing and against accidental loss
g) Images from Wem CCTV will only be considered personal data where they can identify the individual from those images

The GDPR changes some definitions that set the scope of data protection law. The GDPR'S definition of "personal data" is more detailed and makes it clear that information such as an online identifier, for example a computers IP address, can be personal data. It includes additional safeguards for "sensitive personal data."

2.2 The Protection of Freedoms Act 2012

Wem Town Council is considered a "relevant authority" for the purposes of the above act. The CCTV system will comply with the Surveillance Camera Commissioner's code of practice. The 12 guidance principles are as follows: *(text in blue italics is Wem Town Council's action which complies with that guideline)*

CCTV Guidance Principals	*Action by Wem Town Council*
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 reasons for the use of the cameras is stipulated at 1.2 above*
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	*Privacy Impact Assessments for Wem CCTV to be drafted 2019*
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	*Town Centre Signs to be renewed 2019*
There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used	*Town Clerk oversees CCTV system*

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	*Protocols in place for use by West Mercia Police – no other access allowed without permission of Town Clerk*
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	*Images stored for 28 days unless downloaded following approval of request to download images - suck a request can only be approved by Town Clerk or in her absence Assistant Clerk*
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	*Wem Town Council office is secure and access is only avialiable to Town Clerk and Assistant Clerk. Wem SNT also have access to the office subject to clear protocls*
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	*Town Clerk and Assistant Clerk have received guidance in the operation of the system.*
Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use	*Town Council office is secure and access is limited to Town Clerk and Assistant Clerk.*
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	*Wem CCTV is overseen by the Amenities and Services Committee*
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	*No action*
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	*The Town Clerk can liaise with Wem SNT to ensure that the installation of any new CCTV Camera is also supported by up to date police data*

2.3 Introduction to Wem Town Council Code

2.3.1
The Code applies to all public place CCTV schemes and similar surveillance equipment used for monitoring and recording images from those areas to which the public have largely unrestricted access. These include roads, car parks, waiting areas, some parts of shopping areas and access ramps within the camera area.

2.3.2
Wem Town Council, West Mercia Police or other authorised agencies using the system for **specialised and intrusive covert surveillance** will require th**e** appropriate authority to be obtained. Where it is necessary to carry out "Directed Surveillance" under the Regulation of Investigatory Powers Act 2000, the appropriate

authority will be obtained from the Town Council. Any application to carry out Directed Surveillance must be made to the Town Clerk.

2.3.3
This code of practice will be revised when necessary to take into account the following:

- The interpretation of the provisions of the Data Protection legislation
- The changes in technology involved in recording images
- The use of such technology
- Other legislation introduced to cover the use of CCTV

Full consultation will take place when such changes are necessary.

2.4 Scope of the Wem Town Council Code

2.4.1
The Code sets out a number of principles, which must satisfy the conditions of the 2018 Data Protection Act and the Protection of Freedoms Act 2012.

In addition to the 12 points above, the Data Controller will undertake the following:-

1. Identify the person(s) or organisation(s) legally responsible for the management and operation of the scheme
2. Assess the appropriateness of and reasons for using the CCTV or similar surveillance equipment. (see section 1.2 above)
3. Define the purpose and objectives of the scheme (first and second Data Protection Principles)
4. Notify the Information Commissioner in writing of the above information
5. Ensure the scheme and operation complies with the Human Rights Act 1998
6. Maintain appropriate records to facilitate the running of the scheme
7. Define and maintain an Operating Procedure Manual.

2.5 Positioning of Cameras

2.5.1
The location of cameras and the means by which images are captured must comply with the first data protection principle (fair and lawful collection of data (images).

2.5.2
Cameras should be situated where they will capture images relevant to the purpose for which the scheme has been established. (see section 1.2 above) For example, if a camera is located for the prevention and detection of crime, it should be capable of capturing facial images.

2.5.3
Individual Camera siting should take place on the basis of an operational requirement setting out the scope of each camera.

2.5.4
Cameras should be sited in such a way as to monitor only those areas to which the public have access. However, if it is not possible physically to prevent cameras from viewing private areas (for example by blanking out an area) then staff must be suitably trained and made aware of the privacy implications under the Data Protection Act 2018, Human Rights Act 1998 and Sexual Offenders Act 2003 (Voyerism)

2.5.5
Areas required to be viewed by CCTV for security, Royal Protection or similar purposes, which the public do not have access to, are not governed directly by this code. Cameras sited for covert use are operated under the Regulation of Investigatory Powers Act 1998.
However, material gathered for any subsequent proceedings should be dealt with in accordance with the instructions set out in the Operating Procedures Manual.

2.5.6
Signs will be placed in the proximity of the scheme so that the public is aware they are entering a zone covered by surveillance equipment. (see exception clause below) The signs will be clearly visible to the public, be an appropriate size and contain the appropriate information;

2.5.7 (Exception Clause)
In exceptional circumstances, signs may not be placed. In this case, the owners/operators must have assessed (and documented) that they have;

a) Identified a specific activity (for example illegal ticket selling)
b) Identified the need to use surveillance to obtain evidence of that criminal activity (e.g. misuse of illegal drugs)
c) Determined that the use of the signs would prejudice success in gathering that evidence
d) Assessed how long the monitoring should continue to avoid unnecessary observation.
e) Obtained the requisite permission for such surveillance (see section 1.3.2 above)(if this becomes directed surveillance)

2.5.8
Information (data/images) so obtained must only be obtained for the prevention and detection of criminal activity, or the apprehension and prosecution of offenders. It should not be retained for any other purpose.

2.5.9
If the equipment has sound recording facilities, this should **not be used** to record conversation between members of the public in public areas.

2.6 Quality of Images

2.6.1
It is essential that images recorded by the equipment be of sufficient quality to be effective for the purposes for which they are made. It is essential that cameras positioned for crime detection and/or prevention should be capable of good quality images able to identify suspect and offenders and cameras used for crowd safety can identify possible risks and hazards.

2.6.2
The Scheme will have an appropriate maintenance regime so as to maintain this quality. Cameras that fail to reach the appropriate level of quality will be changed or removed from the system. Suitable safeguards will exist to prevent cameras from being tampered with or vandalised. (see operating procedures).

2.6.3
The recording will be by means of a *digital video system*, and recording criteria will be set by agreement with engineers and the system manager.

2.6.4
The period of image retention will be set by the Data Controller, but is generally agreed to be no longer than is necessary for the purposes of the scheme in keeping with the Data Protection Act 2018.

2.6.5
If the system records details of the camera location, date and time etc. then these details will be accurate in order to add to the evidential quality and integrity. The operating procedure manual sets out a documented procedure to ensure the maintenance of these details.

2.7 Processing Images

2.7.1
Images will not be retained for longer than is necessary. Generally, evidential images will be retained under the rules of the Criminal Procedures and Investigation Act 1996. This includes unused material. Full guidelines are set out in the Operating Procedure Manual.
Where images are retained, it will be in accordance with the objectives set out in this code of practice at section 1.2 above.

2.7.2
Images retained for these purposes will be securely stored so as to ensure their integrity is maintained. This will also ensure that the evidential value is maintained and to protect the rights of members of public who may have been recorded.

2.7.3
Access to these images will be carefully controlled and restricted to those persons who are authorised to have access.

2.7.4
Images will only be released to those persons who have a legal right to view them.
Refer to the National Guidelines on release of data to third parties section 2.8 of these codes.

2.7.5
Once the retention period has expired, images not retained for evidential purposes will be deleted from the system.

2.7.6
Images removed for evidential purposes (including those viewed as part of an enquiry but which do not contain evidential images) will be retained in a secure and suitable environment.

2.7.7
Images removed for evidence will be documented fully in the recording log

a) The date on which they were downloaded, copied and by whom
b) The reason they were downloaded
c) Any crime or other unique reference number for cross reference purposes
d) Where the image is stored or to whom it was handed
e) The details and signature of the person taking it from the monitoring room, upon completion of the appropriate register.

2.8.7 Security

2.8.1
Security of Images in general is essential and must be maintained at all times to comply with the Data Protection Act 2018

2.8.2
Access to monitors will be restricted to Town Clerk, Assistant Clerk and other authorised persons.

2.8.3
Access to recorded images will be restricted Town Clerk or in her absence the Assistant Clerk will decide whether to allow requests from third parties in accordance with the documented disclosure policies. See 2.9 below.

2.8.4
During viewing of images by third parties. It is essential that no general access is permitted to other employees and staff unless performing duties in accordance with CCTV monitoring and management. The basis for this restriction is to protect the privacy rights of members of the public and to avoid compromising persons who view the monitors.

2.8.5
Removal of recorded images will be documented and will include the following:-

a) Date and time of removal
b) Name of person/s removing
c) Name of person/s viewing, including any third parties
d) Reasons for the viewing
e) Outcome of the viewing
f) Details of any copies made (location of discs and ref. numbers etc.)
g) Date and time returned to system.

2.8.6
All employees with access to images will be aware of the procedures for image management and limitations of access to images.

2.8.7
All staff with access to the CCTV system will be trained in their responsibilities under this Code of Practice. They should be aware of:-

a) Security Policy for monitoring and image control
b) Disclosure policy (see Access and Disclosure below)
c) Rights of individuals in relation to personal data. (images of those individuals)

2.9 Access To and Disclosure of Images to Third Parties - This section is based on the National Standards for the Release of Data to Third Parties. Most usage of CCTV will be covered by the Data Protection Act 2018. This gives rights to people to see information held about them including CCTV images or images which provide information about them such as car number plates.

Primary Request to View Data

a) Primary 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 proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.);
- Providing evidence in civil proceedings or tribunals
- The prevention of crime
- The investigation and detection of crime (may include identification of offenders)
- Identification of witnesses

b) Third parties, who should be required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- Police (1)
- Statutory authorities with powers to prosecute, (e.g. Customs and Excise; Trading Standards, etc.)
- Solicitors (2)
- Plaintiffs in civil proceedings(3)
- Accused persons or defendants in criminal proceedings (3)
- Other agencies, (which should be specified in the Code of Practice) according to purpose and legal status(4).

c) Upon receipt from a third party of a bona fide request for the release of data, the scheme owner Wem Town Council should:

- Not unduly obstruct a third party investigation to verify the existence of relevant data.

- Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena, (it may be appropriate to impose a time limit on such retention which should be notified at the time of the request).
- NB a time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (e.g. a time limit was about to expire).

d) In circumstances outlined at note (3) below, (requests by plaintiffs, accused persons or defendants) the scheme owner, (or nominated representative) should:

- Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation.

- Treat all such enquiries with strict confidentiality.

Notes

1. The release of data to the police may not be restricted to the civil police but could include, (for example) British Transport Police, Ministry of Defence Police, Military Police, etc. (It may be appropriate to put in place special arrangements in response to local requirements).

2. Aside from criminal investigations, data may be of evidential value in respect of civil proceedings or tribunals. In such cases a solicitor, or authorised representative of the tribunal, should be required to give relevant information **in writing** prior to a search being granted. In the event of a search resulting in a requirement being made for the release of data, such release will only be facilitated on the instructions of a court order or subpoena. (It may be considered appropriate to make a charge for this service. In all circumstances data will only be released for lawful and proper purposes).

3. There may be occasions when an enquiry by a plaintiff, an accused person, a defendant or a defence solicitor falls outside the terms of disclosure or subject access legislation. An example could be the investigation of an alibi. Such an enquiry may not form part of a prosecution investigation. Defence enquiries could also arise in a case where there appeared to be no recorded evidence in a prosecution investigation. The Data Controller will decide each case on its merits.

4. The scheme owner should decide which (if any) "other agencies" might be permitted access to data. Having identified those ‘other agencies’, such access to data will only be permitted in compliance with this Standard.

5. A Data Controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify a reasonable time and accuracy (could be specified in a ½ hour period). There is no longer a £10 fee for straight forward requests, but a reasonable charge can be made under the 2018 Data Protection Act for complicated and time consuming requests.

Secondary Request to View Data

a) A 'secondary' request for access to data may be defined as any request being made, which does not fall into the category of a primary request. Before complying with a secondary request, the scheme owner should ensure that:

- The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection, section 163 Criminal Justice and Public Order Act 1994, etc.);

- Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act);

- Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and

- The request would pass a test of 'disclosure' in the public interest. (see note one below)

b) If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards should be put in place before surrendering the material:

- In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice. (see note 2 below.)

- If the material is to be released under the auspices of 'public well-being, health or safety', written agreement to the release of material should be obtained from of Wem Town Council. The member of staff should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice.

c) Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

Notes

(1) 'Disclosure in the public interest' could include the disclosure of personal data that:

i) provides specific information which would be of value or of interest to the public well being

ii) identifies a public health or safety issue

iii) leads to the prevention of crime

(2) The disclosure of personal data which is the subject of a 'live' criminal investigation would always come under the terms of a primary request, (see Section 2.8 a) above).

2.10 Individual Subject Access under Data Protection legislation

2.10.1

a) Under the terms of Section 7 of the Data Protection Act 1998, individual access to personal data, of which that individual is the data subject, must be permitted providing:

- The request is made in writing;
- A fee is no longer required for each individual search
- The Data Controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request;
- The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information, which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances it is suggested that within one hour of accuracy would be a reasonable requirement);
- The person making the request is only shown information relevant to that particular search and which contains personal data of her or himself only, unless all other individuals who may be identified from the same information have consented to the disclosure;

b) In the event of the scheme owner complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.

c) The owner is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided, (However every effort should be made to comply with subject access procedures and each request should be treated on its own merit).

d) In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

- Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation;
- Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings;
- Not the subject of a complaint or dispute which has not been actioned;
- The original data and that the audit trail has been maintained;
- Not removed or copied without proper authority;
- For individual disclosure only (i.e. to be disclosed to a named subject)

2.10.2

The right of access to images of individuals by that individual is provided for in section 7 of the Data protection Act 1998 and should be afforded wherever possible.

2.10.3

All staff must be able to recognise a request for access to recorded images by data subjects.

2.10.4
Data subjects will be provided with a standard subject access request form that:-

a) Indicates the information required to locate the images requested
b) Indicates the information required to identify the person making the request
c) Indicates the circumstances when a fee will be required (a standard fee is no longer charges for straight forward cases)
d) Asks whether the individual would be satisfied with merely viewing the images recorded
e) Indicates that a response will be made promptly and **no longer than 30 days** from the day the request was received (which will be endorsed on the form)

2.10.5
Individuals will be provided information describing the types of images recorded and retained, the purpose for which those images are recorded and retained and information about the disclosure policy in relation to those images.

2.10.6
All subject access requests will be dealt with by the Town Clerk or Assistant Clerk. Where possible, the designated member of staff will locate the images requested.

2.10.7
Town Clerk or Assistant Clerk will determine whether disclosure to the individual will entail disclosing images of third parties. Similarly, he/she will decide if the images are held under a duty of confidence. It is likely that member of the public walking in a public area will have less expectation that their images are held under a duty of confidence than those recorded for example in a rest area or toilet queue.

2.10.8
If third party images are not to be disclosed, they should be disguised or blurred out as set out above 2.10.1. (b)

2.10.9
If the coordinator or designated member of staff decides that a subject request form should not be complied with, he/she will document fully the following:-

a) The identity of the individual making the request
b) The date of the request
c) The reason(s) for refusing to supply the images requested (see 2.9.10 below)
d) The name and signature of the coordinator or designated member of staff making the decision.

2.10.10
All staff should be aware of the individuals' rights under this section of the Code of Practice. (Seventh data protection principle)

2.10.11
Where the Town Clerk or Assistant Clerk refuses to supply a subject with a copy of data, the reason should be one of the following:-

1. Images of third parties would be supplied at the same time, but without their permission and it would breach a duty of confidentiality to supply them and it is not possible to contact them and obtain that permission.
2. The supply of images would prejudice a criminal investigation.
3. The applicant has not provided sufficient information to prove his/her identity.
4. Providing them would involve disproportionate effort.

2.11 Other Individuals' Rights

The disclosure or viewing of images may cause third parties to be compromised. The Data Protection Act 2018 makes provision for other individuals' rights to be taken account of. Section 94(6) and 95(5)of the Act provides an individual the right to prevent processing which is likely to cause damage or distress. Operators and managers must have a clear understanding of these rights to avoid leaving the data controller and operators open to civil litigation.

The following standards apply;

2.11.1
All staff must be able to recognise a request from an individual in order to;

a) Prevent processing likely to cause substantial and unwarranted damage to that individual
b) Prevent automated decision taking in respect of that individual[1]

2.11.2
All staff must be aware of the coordinator or designated member of staff who is responsible for responding to such requests

2.11.3
The coordinator or designated member of staff will:-

a) Document fully any response to a request where processing is likely to cause damage or distress and whether it will be complied with or not.
b) Provide a written response to the individual within 21 days setting out the decision and reasons
c) Retain a copy of the response to the individual
d) If an automated decision is made about an individual, notify the individual in writing of that decision
e) Where an appeal has been received in writing to an automated decision within 21 days of having been notified of the decision, he/she will reconsider the decision.
f) If such an appeal is received, then again within 21 days a response will be made setting out the steps being taken to deal with the individuals' appeal.

2.11.4
The manager or designated member of staff shall document the following:-

1) The original decision
2) The request from the individual
3) The response to the request from the individual

2.12 Compliance with Code of Practice

2.12.1
All CCTV schemes operated by Wem Town Council will comply with this Code of Practice. There will be a system of monitoring in place to ensure:-

a) compliance with the codes
b) public confidence is maintained
c) continued ethical use of the system

[1] Automated decision taking is defined later in this code, but an example would be a speed camera

d) best value is obtained

2.12.2
In accordance with the Surveillance Camera Commissioner Code (Principle 10), a regular audit and review will be carried out by Wem Town Council as owners of the CCTV system. This report will be made public.

2.12.3
The contact point indicated on the signs within the area covered by CCTV will be available to members of the public at least during office hours.

1) A copy of the code of practice
2) Subject access request forms
3) Details of the complaint procedure (set out in the operating procedure manual)[1] should they have concerns about the use of the system
4) Details of the complaint procedure to be followed where they may have concerns about non-compliance with the provision of this code.

2.12.4
The complaint procedure will be fully and clearly documented (see operating manual) and a record of all complaints received will be maintained. These records should be taken into account when assessing the effectiveness of the overall scheme.

2.12.5
A report reviewing complaints will be provided for the data controller(s) in order that compliance with legal obligations and provisions with this code of practice can be monitored.

3.0 Technical Standards

3.0.1
The CCTV scheme operated by Wem Town Council will carry out an annual assessment of the cameras. This should be done in conjunction with any operational requirement specification for each camera and the home office recommendations for CCTV design. (Principle 3 Data Protection Act 2018– Data collected in an adequate and relevant manner – refers to quality of cameras)

3.0.3
Where technical improvements can be made to improve the operational effectiveness of the scheme, recommendations will be documented and submitted to the Town Council for consideration and discussion.

3.0.4
If it is apparent that environmental changes are required, then the data controller will contact those departments responsible for the environment to discuss how changes can be made to improve the operational effectiveness of the scheme.
e.g. Trees obscuring camera views may need pruning. This process should again be documented.

Wem Town Council Contact Details

Wem Town Council
Penny O'Hagan, Town Clerk
Edinburgh House, New Street, Wem, SY4 5DB.
Tel: 01939 232733, E mail: info@wem.gov.uk

[1] Complaints against police officers will be referred to Warwickshire and West Mercia Police