



# **EPPING FOREST DISTRICT COUNCIL**

## **Closed Circuit Television Code of Practice**



**For the operation of public space CCTV systems in the  
Epping Forest District, including re-deployable systems  
Body Worn Video, Unmanned Aerial Vehicles & Council owned buildings.**

**Epping Forest District Council is a  
Member of NASCAM.**



**Version 3.1  
September 2020  
Owner: Senior Responsible Officer (SRO)**

## Table of Contents

<b>Code of Practice .....</b>	<b>3</b>
1. Introduction .....	3
2. Terms and Definitions.....	3-5
3. Background.....	5
4. Aims of Epping Forest District Council's CCTV.....	5
5. Purposes of Epping Forest District Council's CCTV .....	5
6. Council CCTV Objectives .....	6
7. Revision and Alterations to the Code of Practice .....	6
8. Planning of CCTV Systems .....	6-7
9. Aerial Camera Usage .....	7
10. Body Worn Cameras.....	7
11. Mobile Cameras.....	7
12. Dummy Cameras .....	7
13. Ownership/Copyright Issues.....	7-11
14. Capture, Protection and Storage of Data .....	11
15. Cataloguing of Downloaded Discs .....	12
16. Erasure of Recorded Images.....	12
17. Storage/Destruction of Transferred Images.....	12
18. Use of Audio.....	12
19. Police Use of Recorded Images (Including Point of Transfer).....	12-13
20. Provision of Recorded Stills.....	13
21. Epping Forest District Council Viewing of Recorded Images .....	13
22. Evaluation, Monitoring and Audit of Scheme .....	13-14
<b>Appendices .....</b>	<b>15</b>
Appendix 1. EFDC CCTV Locations & Camera Numbers.....	15
Appendix 2. Epping Forest District Council CCTV Sign .....	16
Appendix 3. Epping Forest District Council Re-Use of Public Sector Information Policy .....	17-20
Appendix 4. Epping Forest District Council – Aerial Camera Usages Policy .....	21-23
Appendix 5. Epping Forest District Council Policy For Body Worn Cameras .....	24-31

# **Code of Practice**

## **1. INTRODUCTION**

This Code of Practice is to control the management, operation and use of all Closed-Circuit Television (CCTV) systems under the control of Epping Forest District Council and is used in conjunction with the Home Office Surveillance Camera Code of Practice pursuant to section 29 of the Protection of Freedoms Act 2012.

Epping Forest District Council own and operate large numbers of public space CCTV schemes, these work independently throughout the district.

The Council will retain ownership of all recorded material in various formats, including, Compact Disc (CD), Digital Versatile Disc (DVD) Universal Serial Bus (USB), external HDD and hard copy print, and retains absolute copyright of any recorded material. For the purpose, of this document, any recorded material will be referred to as 'video imagery'. The Council will not release video imagery for commercial purposes or for the provision of entertainment. Video imagery will only be released for the purposes of evidence and on occasions education and training purposes.

The day-to-day operation of the Council's systems will be the responsibility of the Community Resilience Team within the Community and Partnerships service. The CCTV systems operate 24 hours a day, 365 days a year, except in cases of maintenance/upgrades, faults etc, where it may be necessary for a particular system to be powered down for a period of time.

The Community Resilience team will supervise the code and ensure its implementation.

It is a condition of acceptance as a partner that users of CCTV demonstrate commitment to operate in accordance with this code by signing the required Certificate of Agreement in this document. Each participant in the scheme is bound by this Code of Practice and any subsequent amendments thereto.

## **2. TERMS AND DEFINITIONS**

For the purposes of British Standards the terms and definitions given in BS EN 62676 suite of standards apply, together with the following.

### **CCTV Scheme**

Totality of arrangements for CCTV in a locality including but not limited to the technological system, staff and operational procedures.

### **Observation Mode**

Mode of operation of a CCTV system, whereby monitoring is carried out live, the sole purpose of which is to observe the images in real time and not to record, store, or print the information viewed.

### **Retrieval System**

A CCTV system having the capability in any medium of effectively capturing data that can later be retrieved, viewed or processed.

### **CCTV System**

Surveillance items comprising of cameras and all associated equipment for monitoring, transmission and controlling purposes, for use in a defined area.

### Distributed System

Sub system, any part of which may be linked temporarily or permanently for remote monitoring within the CCTV system.

### Data

All information collected by the CCTV systems, including personal data.

### Incident

An activity that has been identified as an offence that has been committed or an occurrence that has taken place that warrants further specific action from either the Police or from the Council or other third parties as the Council sees fit such as Insurance companies or solicitors. For the purposes of this scheme an incident is defined as:

**Any event or occurrence monitored by a controller/system in respect of which information needs to be passed to another source to generate a response.**

OR

**A request by an authorised persons or body to monitor specific events or activity in accordance with the purposes and key objectives of the scheme.**

The provisions of the Regulation of Investigatory Powers Act (RIPA) 2000 may be relevant to such requests.

### Owner

Legal person or entity, agency or individual designated and trained as having direct responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme.

### Manager

The CCTV Operations Officer has direct responsibility for the implementation of the policies, purposes and methods of control of a CCTV scheme, as defined by the owner of the scheme.

### Supervisor

Person specifically designated, trained and authorised by the owner of a scheme to ensure that at all times the system is operated in accordance with the Code of Practice and any procedural instruction issued by the owner or manager.

### Operator

Person specifically designated and authorised by the owner of a CCTV scheme to carry out physical operation of controlling that system.

### Recording Material (e.g. CD/DVD/USB)

Any medium that has the capacity to store data, and from which data can later be recalled, irrespective of time.

### Recorded Material

Any data that has been recorded on any medium that has the capacity to store data and from which data can later be recalled irrespective of time.

### Hard Copy Print

Paper copy of a still image or images which already exist on recorded material.

### Privacy Masking

The common term covering the need to restrict what can be seen by means of CCTV. It applies equally to images displayed in real time for surveillance purposes and images recorded for later use.

### Directed Covert Surveillance

This is defined under section 26 of the Regulation of Investigatory Powers Act (RIPA) 2000. It relates to covert surveillance for specific purposes where the gathering of private information is a likely outcome.

## **3. BACKGROUND**

Epping Forest District Council has and is continuing to install CCTV systems some of which are capable of expansion. Cameras have been installed within specific target areas which have been identified through the gathering of information, including the use of local public information, Crime Pattern Analysis and the Council's CCTV Decision Matrix tool.

Community Safety is defined as any intervention that deals with anti-social behaviour and fear of crime, which may affect the quality of life of individuals and the local community. The Crime and Disorder Act 1998 defines anti-social behaviour as behaviour which causes, or is likely to cause alarm, harassment or distress to one or more persons not of the same household.

## **4. AIMS OF EPPING FOREST DISTRICT COUNCIL'S CCTV**

- Help secure safer areas and environments for those who visit, work in, trade in or enjoy leisure pursuits within the district.
- The Council's CCTV schemes will be operated fairly and lawfully and will only be used for the purposes for which they were established, or subsequently agreed in accordance with this code.
- The Council will regularly monitor, review and enhance its CCTV schemes in order to ensure and improve their effectiveness.

## **5. PURPOSES OF EPPING FOREST DISTRICT COUNCIL'S CCTV**

Epping Forest District Council's CCTV schemes exist for us to record, view, and occasionally monitor activity within the intended area of coverage. Safeguards are used within the systems' capabilities to ensure cameras cannot be focused within private areas, such as windows, where there is no public access. Where it is unavoidable to have a camera focused on a home or other private area as part of a larger point of focus, privacy masking will be used to cover the private area from view. This will minimise collateral intrusion.

## **6. COUNCIL CCTV OBJECTIVES**

- The introduction of a central hub for all EFDC CCTV matters. (Based within the Community Resilience section), also referred to as a SPOC (Single Point of Contact)
- Manage our CCTV responsibly by providing a compliant delivery of service through the implementation of robust CCTV processes and guidelines.
- Provide high quality evidence which may be used to further an investigation by the Council or third parties as well as law enforcement agencies to prosecute offenders.
- Assist in the reduction and prevention of crime and increase public confidence.
- All schemes to be made 'fit for purpose' through preventative and reactive maintenance plans and regular operational requirement reviews.

- Effectively manage the public and third-party perception of CCTV including ‘unrealistic expectations’
- Monitor environmental conditions.
- To provide transparency to the public on how, why and where CCTV is being utilised, successes and outcomes along with other information members of the public may wish to know. Much of our CCTV information can be readily found through our Council’s CCTV website page.

Every effort is made in the planning and design of the Council’s CCTV systems to provide maximum effectiveness within the current area of coverage or such additional areas which may subsequently form part of the system. It is not possible to guarantee the system will be able to see or provide evidence for every incident that may occur within the target area.

## **7. REVISION AND ALTERATIONS TO THE CODE OF PRACTICE**

This Code of Practice will be regularly reviewed, and any required revisions and alterations will then be made.

## **8. PLANNING OF CCTV SYSTEMS**

In planning the installation of CCTV systems, Epping Forest District Council refers to a number of standards and documents in order that the passport to compliance is adhered to.

### Locations of cameras (See appendix 1)

All locations where cameras are to be installed will be assessed using various relevant statistics and analysis gathered from various sources, including the Police, local communities and local businesses to ensure maximum effectiveness and productivity.

### Signage (See appendix 2)

Corporate signs will be installed in and around the areas covered by the Council’s CCTV systems. The placing of such signs is an important aspect of the principles of the Data Protection Act 1998. They will be of an appropriate size to the location and will contain the following information:

- a) The purpose of the scheme
- b) What the Council intends to do with the information gathered i.e. prosecute offenders
- c) Who owns the scheme
- d) Contact details
- e) Carry relevant Council logo/s and CCTV symbol

The signs will read, or variations of this type:

*“CCTV cameras are in operation 24 hours a day.  
Images are being recorded for the purpose of public safety, crime prevention and detection.  
Evidence gathered may be used to prosecute offenders.  
This scheme is controlled by Epping Forest District Council  
Tel: 01992 564608”*

*“CCTV 24 hr video recording.  
Images are being recorded in this area for the purpose of building security, staff and public safety.  
Evidence gathered may be used to prosecute offenders.  
This scheme is controlled by Epping Forest District Council  
Tel: 01992 564608”*

## 9. AERIAL CAMERA USAGE

Epping Forest District Council has two Aerial Camera Systems available for use by all within Community and Partnership for aerial survey purposes. A policy has been published relating to usage of these systems (see appendix 4). In addition, any personnel involved in the flight or use of these systems must adhere to the operational instructions and procedures laid out in the Council's **Flight Operations Manual**.

## 10. BODY WORN CAMERAS

The use of Body Worn CCTV can be beneficial in a number of ways. It can be used to instantly record incidents, act as a visible deterrent to verbal and physical abuse towards officers, provide evidence to support internal or other investigations and strengthen accountability and transparency. The Council's **Body Worn Camera Policy** (see appendix 5) provides users and supervisors with the guidance they require to ensure that the use of Body Worn Cameras complies with the relevant legislation.

## 11. MOBILE CAMERAS

Rapid Deployment Surveillance Camera/s are more temporary in nature and can be moved from site to site. The purpose of these systems is to; Help to prevent, detect and reduce criminal activity and anti-social behaviour. Help make Epping Forest District safe for those people who live, work, trade and visit the district. Help authorities and agencies in the performance of their statutory enforcement powers. To identify, apprehend and prosecute offenders by providing evidential material for any lawful process or court proceedings. The camera/s are a limited resource and designed to give a supportive and rapid response to hotspots of crime and ASB on a temporary basis across the District.

There must be sound and specific evidence to show that the camera/s are an appropriate response. This will need to be measurable by recorded incidents/offences, repeated complaints of past incidents, or substantiated intelligence on future incidents. Each deployment application typically is deployed for up to 3 months. It may be kept in situ longer should the criteria for proportionality and justification be met. Epping Forest District Council will make the final decision on all deployments. Cameras will not be deployed without prior written authority from Epping Forest District Council namely The CCTV Operations Officer or appointed representative.

## 12. DUMMY CAMERAS

In the past, Epping Forest District Council has used dummy cameras in some locations within the district. However, studies have shown that public confidence in CCTV is based upon effectively operating cameras, and therefore dummy cameras will no longer be used within any CCTV schemes operated by the Council.

## 13. OWNERSHIP/COPYRIGHT ISSUES

Epping Forest District Council's CCTV schemes are registered under the Data Protection Act 1998. The registration number is **Z5033101**. The Data Controller is Epping Forest District Council. All data will be processed in accordance with the stated purpose ensuring compliance with the Act.

### CCTV - Primary request to view data

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.
- 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.

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

- Police.
- Statutory authorities with powers to prosecute, (eg. Customs and Excise; Trading Standards, etc).
- Solicitors.
- Claimants in civil proceedings.
- Accused persons or defendants in criminal proceedings.
- Insurances
- Other agencies, (as agreed by the Data Controller and notified to the Information Commissioner) according to purpose and legal status.

Upon receipt from a third party of a bona fide request for the release of data, the data controller shall:

- 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. A time limit shall be imposed on such retention which will be notified at the time of the request.

Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller or nominated representative shall:

- 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.

### CCTV - Secondary request to view data

For example, where a member of the public requests CCTV images of their vehicle in a car park where there has been an incident of criminal damage or a fail to stop incident.

Before complying with a secondary request, the data controller shall ensure that:

- The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection Act 2018, Human Rights Act 1998, 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 2012); Protection of Freedoms Act 2012.
- Due regard has been taken of any known case law (current or past) which may be relevant, (eg. R v Brentwood BC ex p. Peck);
- The request would pass a test of 'disclosure in the public interest'.

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards shall 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.

- 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 a senior officer within the Local Authority. The officer 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.

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.

### CCTV - Individual Subject Access under Data Protection Legislation

Under the terms of Data Protection legislation, individual access to personal data of which that individual is the data subject must be permitted providing:

- The request is made in writing;
- The data controller is supplied with sufficient information to satisfy him or her self 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.

In the event of the data controller 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).

The data controller 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.

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).

### CCTV Retrieval & Point of Transfer (POT) Fees

CCTV requests are chargeable with the exception of law enforcement agencies such as the Police.

Fees:

£120.00 for up to first 4 hours of CCTV footage.

Fee includes labour time, statements, sundries, storage media, secure delivery and all administration.

After the initial 4 hours there will be an hourly rate charge of £30 per hour or part hour to cover officer time. As per EFDC's re-use of public sector information policy. (Last reviewed July 2019)

E.g.: request for 5hrs 25mins of footage  
£120.00 + £60 = £180.00

Payment: (Raising a sundry debtor using the AIMS system)

Requester is required to provide:

Name  
Address  
Post Code  
Ref No.

Copy of CCTV to be retained on record by EFDC in accordance with data storage and destruction procedures set out in EFDC CCTV Code of Practice.

VAT N/A (Non-business).

### CCTV - Procedure for the release of evidence

The Council is committed to the belief that everyone has the right to respect for his or her private and family life. Although the use of CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (data) which the system gathers.

After considerable research and consultation, a nationally recommended standard has been adopted by the Council.

All requests for the release of data shall be channelled through the data controller or his/her nominated representative.

### CCTV - Process of disclosure

Replay the data to the requester only, (or responsible person acting on behalf of the person making the request).

The viewing should take place in a separate viewing booth/room and not in the control or monitoring area. Only data that is specific to the search request shall be shown.

It must not be possible to identify any other individual from the information being shown, (any such information will be blanked-out, either by means of electronic screening or manual editing on the monitor screen).

If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material shall be sent to an editing house for processing prior to being sent to the requestee.

For complaints about the use of the Council's CCTV scheme, refer to section 1.

## **14. CAPTURE, PROTECTION AND STORAGE OF DATA**

System operators should adopt the 12 guiding principles under the Home Office's Surveillance Camera Code of Practice.

Because of differences in some of our CCTV systems, image retention periods on systems differ. All new systems and upgraded systems (2019 onwards) will retain images for 31 days as a maximum period available for download.

Whichever medium is chosen for the capture and initial storage of images, effective means are made available for transferring the images to the computer system where they are able to be used and possibly archived.

Images on reusable media should be copied from the original storage medium in the original file format onto a secure media. This secure media could be Write Once Read Many (WORM) or secure network storage. The term 'secure server' should be taken to mean an environment, including a security management system, which is accredited to a level of at least 'OFFICIAL' under the Government Classification Scheme (GCS). Once the images and associated data have been copied onto the secure media, they cannot be overwritten or altered.

The generation of the secure copy will be carried out as soon as possible after the capture to reduce the time and opportunity for the accidental or malicious alteration to images.

All imagery master or working copies will be appropriately identified in order to facilitate the storage, retrieval and eventual disposal of case material.

Any downloaded data exhibited in Court as evidence must be the Master Copy. There must be no editing or recording from other sources on to the master copy. However, while the master copy is in Police possession, the Police may take one working copy of the disc and a second copy of the disc to be used as disclosure material to the defence. Written statements will be required from the Police Officers as supporting evidence on copying and other handling of the transferred images onto the disc.

As a rule, unless requested the Council does not keep a copy of the requested CCTV.

The software required for viewing proprietary formats will be made available to avoid images being inaccessible. Replay software will be provided with each recording to assist with the correct viewing of the files in their native format.

Working copies can be in many forms. The files will be copied onto any suitable medium or distributed electronically using a secure system only for circulation to the Investigating Officer or Crown Prosecution Service.

Those that are retained for evidential purposes must be retained in a secure place to which access is controlled such as a secure safe.

## **15. CATALOGUING OF DOWNLOADED DISCS**

Data downloaded to any storage medium will be given a unique reference number and recorded in the CCTV data request register.

The data will then be stored securely at the Civic Offices in Epping until collected by the Investigating Officer or representative.

## **16. ERASURE OF RECORDED IMAGES**

Any recording made on the Council's CCTV systems will be automatically overwritten by the server after a set period of time. This will be any time period between 14 and 31 days, depending on the individual system itself.

## **17. STORAGE/DESTRUCTION OF TRANSFERRED IMAGES**

Transferred images will be stored securely to ensure that there is no unauthorised access or possibility of accidental or intentional damage. The storage space should be kept dust and moisture free and kept at a constant temperature and always kept locked when not in use. Only authorised key holders will have access to the secure area. Images removed from the systems actual storage drive which is then deemed to be of no further use or the requester has not collected the images will after advisement safeguards be destroyed after **one further month** and recorded in the CCTV destruction log. Retention of data can be longer subject to appeals and sentencing for example.

## **18. USE OF AUDIO**

None of Epping Forest District Council's CCTV systems are configured to record any audio activity in conjunction with the video recording except in the case of private interviews within some Council offices and rooms. Signs are clearly displayed and marked where audio is used.

## **19. POLICE USE OF RECORDED IMAGES (Including Point of Transfer)**

When the Police have reasonable cause to believe that an incident has been recorded which involves or may involve criminal activity a duly authorised Police Officer will be handed the downloaded data against signature and in accordance with the strict procedures in place.

A 'point of transfer' will be established in which the responsibility of data transfer handling to the Police. That point of transfer will depend on the nature of the images being transferred, the recording format and equipment used by Epping Forest District Council. At whatever stage this point of transfer occurs the Police audit trail must start from that point. Continuity of data handling will be demonstrated throughout, ensuring that the Police audit trail links directly to the Council's audit trail.

The Police have speciality facilities for copying data.

Recorded images owned and managed outside Local Authority Control may require to be processed by copying or the production or reproduction of still images.

The Information Commissioner has approved a process whereby Local Authorities may process data on behalf of a third-party Data Controller for policing purposes.

The process will ensure that the third-party Data Controller, the Data Processor (Local Authority) and the Police will be seen to have made every effort to comply with the seventh principle of data protection law.

At the conclusion of use of any Master or Copy recorded by Police, it may be returned to the Council, unless the Court directs that it should be destroyed instead of being handed back to the owners. In the latter case a certificate of instruction will be provided by the Police to finalise the audit trail relating to those data images.

## **20. PROVISION OF RECORDED STILLS**

The photographic process should only be used to assist in the identification of incidents or in training or for demonstration purposes. Still photographs will not be taken as a matter of routine.

A Police Officer may request the owners to produce still frame images from recordings, also known as snapshots. All such stills will be given a unique reference number and be recorded in the CCTV data request register. A file copy may also be retained in the Civic Offices. All still photographs will remain the property of its owners.

Any still image provided by the Council to the Police will be kept secure and its handling logged in exactly the same way as recorded images. Any stills handed to the Police should be treated on the

basis that they are required in Court. The still image is therefore to be placed in a sealed envelope with an exhibit label attached and a Witness Statement provided.

## **21. EPPING FOREST DISTRICT COUNCIL VIEWING OF RECORDED IMAGES**

A Council staff member may request to view the recording of a specified incident which does not involve or appear to involve criminal activity but which may involve the management services for which the officer is responsible (i.e. Housing, Parking) if the officer has been made aware of an incident through other means and has reason to believe the CCTV may assist them.

- Any private viewings must be first approved by the Data Protection Officer.
- A log will be kept of any such viewings.
- No other viewings by an unauthorised person will be permitted.

## **22. EVALUATION, MONITORING AND AUDIT OF SCHEME**

The scheme owners should arrange for independent evaluation to establish whether the purposes as stated are receiving compliance and whether the objectives are being achieved.

The process should include:

- a) Assessment of the impact on crime the system has had.
- b) Assessment and comparison of neighbouring areas without CCTV.
- c) Views of the public.
- d) Operation of the Code of Practice.
- e) Whether the purposes and key objectives of the system remain valid.
- f) Complaints received relating to the use of the scheme.
- g) Data Protection and legal requirements.
- h) Maintenance schedule and performance test of the systems.

Evaluation should be provided for in annual budgetary considerations.

An Annual Report may be compiled and made available for public information by the Council, or their advisers. The topics covered within the report should include details of the following:

- a) A description of the scheme and the geographical areas of operation
- b) The scheme's policy statement
- c) The purpose and scope of the scheme
- d) Any changes to the operation or management of the CCTV scheme
- e) Any changes that have been made to the policy
- f) Any proposals to expand or reduce the operation of the scheme
- g) The aims and objectives for the next 12 months (CCTV Strategy)

Any Annual Report will also provide details of the schemes' achievements during the previous 12 months, which may be based on information already held by the scheme. The assessment of the schemes' performance should include:

- a) The number of incidents recorded by the scheme
- b) The number of incidents reported to the Police and, where appropriate, other bodies, e.g. the local authority
- c) An assessment of the CCTV scheme's impact on crime levels and types of crime in the area covered by the scheme

# Appendix 1



## EFDC CCTV Locations & Camera Numbers.



	Location Of Cameras	No. Of Cameras	System	Postcode
1	Bakers Lane Car Park, Epping	12	Genie	CM16 5EG
	Bansons Car Park, Ongar (Sainsburys)	8	Genie	CM5 9AA
3	Barrington Hall, Debden (Careline)	3	Hik Vis	IG10 2AY
4	Birch View The Plain, Epping	18	Hik Vis	CM16 6TJ
5	Bobbingworth, (Land Drainage)	14	Hik Vis	CM5 0LL
6	Borders Lane Shopping Parade, Loughton	11	Genie	IG10 3QX
7	Buckhurst Court, Buckhurst Hill (Careline)	4	Hik Vis	IG9 6EH
8	Burton Road, Debden	9	Hik Vis	IG10 3FR
9	Chapel Road, Epping (Careline)	2	Hik Vis	CM16 5EE
10	Civic Offices, High Street, Epping	13	Hik Vis	CM16 4BZ
11	Civic Offices, (Homefield House), Epping	4	Hik Vis	CM16 4BZ
12	Civic Offices, IT Helpdesk + CompSuite, Epping	6	Hik Vis x2	CM16 4BZ
13	Clifton Road, Loughton (Land Drainage)	1	Geo Vis	IG10 1EA
14	Cornmill Car Park, Waltham Abbey	12	Genie	EN9 1RB
15	Community Garden, Cottis Lane	2	Hik Vis	CM16 4BP
16	Cottis Lane Car Park, Epping	16	Genie	CM16 7PX
17	Darby Drive, Waltham Abbey	10	Hik Vis	EN9 1EE
18	Debden Broadway, Loughton	64	Geo Vis x2	IG10 3SP
19	Debden Broadway Housing Office	3	Hik Vis	IG10 3SP
20	Epping Forest District Museum, Waltham Abbey	16	Hik Vis	EN9 1EL
21	Frank Bretton House, Ongar (Careline)	3	Hik Vis	CM5 9BS
22	Grove Court, Waltham Abbey (Careline)	4	Genie	EN9 1BP
23	Hedgers Close, Loughton (Careline)	5	Hik Vis	IG10 1SU
24	Hemnall House, Epping	8	Hik Vis	CM16 4DY
25	Hemnall Street Council Office	4	Hik Vis	CM16 4LZ
26	High Road, Loughton	31	Hik Vis x2	IG10 4BE
27	High Street, Epping	31	DM SD	CM16 4BZ
28	Hill House Shops	16	HikVis	EN9 3EL
29	Hill House Leisure Centre	21	HIKVis	EN9 2BL
30	Hyde Mead House, Nazeing (Careline)	4	Hik Vis	EN9 2HT
31	Jessop Court, Waltham Abbey (Careline)	6	Hik Vis	EN9 3JF
32	Jubilee Court, Waltham Abbey (Careline)	5	Hik Vis	EN9 3JB
33	Leonard Davis Court, North Weald (Careline)	4	Hik Vis	CM16 6BS
34	Limes ANPR, Limes Avenue, Chigwell	2	Vista	IG7 5NX
35	Limes Farm Shopping Parade, Chigwell	14	Hik Vis	IG7 5NT
36	Limes Farm Green Block, Chigwell	32	Genie	IG7 5NQ
37	Limes Farm Red Block, Chigwell	32	Genie	IG7 5LA
38	Limes Farm Yellow Block, Chigwell	20	Genie	IG7 5ND
39	Limes Hall, Limes Farm, Chigwell	22	Hik Vis	IG7 5LP
40	Loughton Way Shopping Parade, Buckhurst Hill	12	Hik Vis	IG9 6AR
41	Lower Queens Road Car Park, Buckhurst Hill	19	Hik Vis	IG9 5BZ
42	North Weald Airfield	21	Hik Vis	CM16 6HR
43	North Weald Shopping Arcade	4	Genie	CM16 6BY
44	Norway House, North Weald (30+15+15)	60	Hik Vis x3	CM16 6BH
45	Oakwood Hill Depot, Loughton	25+6	GeoVis+Hik	IG10 3FQ
46	Parklands Shopping Parade, Coopersale	11	Hik Vis	CM16 7RE
47	Parsonage Court, Loughton (Careline)	7	Hik Vis	IG10 2BB
48	Pelly Court, Epping (Careline)	20	Hik Vis	CM16 4NA
49	Pleasance Car Park, Ongar (Library)	7	Genie	CM5 9AG
50	Pryles Lane Shopping Parade, Loughton	16	Genie	IG10 2NN
51	Quaker Lane Car Park, Waltham Abbey	12	Genie	EN9 1HF
52	Queens Road, Buckhurst Hill	21	DM SD	IG9 5EP
53	Roundhills Shopping Parade, Waltham Abbey	11	Hik Vis	EN9 1UU
54	Shelley Close, Ongar	8	Hik Vis	CM5 0BX
55	Springfields, Waltham Abbey	16	Genie	EN9 1UE
56	Sun Street Library, Waltham Abbey	1	Hik Vis	EN9 1EL
57	Town Mead, Orchard Gardens, Waltham Abbey	12	Hik Vis	EN9 1RS
58	Traps Hill Car Park, Loughton	18	Hik Vis	IG10 1SZ
59	Ongar Police Station	5	Hik Vis	CM5 9AG

<b>Total cameras</b>	<b>804</b>
----------------------	------------

APPENDIX 2

EPPING FOREST DISTRICT COUNCIL CCTV SIGN



This scheme is controlled by  
Epping Forest District Council  
Tel: 01992 564608

## **APPENDIX 3**

### **EPHING FOREST DISTRICT COUNCIL RE-USE OF PUBLIC SECTOR INFORMATION – POLICY**

#### **1. Introduction**

- 1.1. The Re-use of Public Sector Information Regulations 2005, (here referred to as 'the Regulations') came into effect on 1 July 2005. They encourage the re-use of public sector information for which the public authorities listed in the regulations hold the copyright.
- 1.2. These regulations apply to Epping Forest District Council, and this policy sets out how they relate to requests for re-use of information for which the Council holds the copyright.
- 1.3. The Regulations derive from EU Directive 2003/ 98 / EC on the re-use of Public Sector Information, which also came into force on the 1 July 2005.

#### **2. WHAT IS MEANT BY RE-USE?**

- 2.1 When the Council releases information which has been requested under legislation such as the Freedom of Information Act 2000 (FOIA), a person may ask if the information can be re-used, perhaps for commercial purposes. Without permission this might breach the Council's copyright. The regulations are concerned with this management of such re-use.
- 2.2 Nothing in the Regulations affects rights of access under other legislation, such as the FOIA, Environmental Information Regulations (EIR) or the Local Government Acts.

#### **3. WHAT ARE THE BASICS OF THE REGULATIONS?**

- 3.1 The Council is not obliged under the regulations to make public sector information available for re-use. However, if the Council decides to do so this has to be done in accordance with the Regulations.
- 3.2 Thus the Regulations provide for:
  - (a) a 20 working day period (beginning from the first working day after the request is received) for the Council to respond to a request for re-use, although this period may be extended where the information requested is extensive or complex;
  - (b) a licence fee if re-use is not to be free;
  - (c) a licence must not restrict competition;
  - (d) exclusive licensing arrangements will not be allowed except for the provision of a service in the public interest and such arrangements shall be published.
  - (e) The Council must make available to the public any conditions and any standard charge for re-use;

- (f) Information for re-use must be made available by the Council electronically where possible and appropriate; and
- (g) The Council must not discriminate between different applicants making requests for re-use for comparable purposes.

#### **4. COPYRIGHT**

- 4.1 The Regulations do not affect the Council's copyright.
- 4.2 The supply of documents (for example under the FOIA) does not give any person a right to re-use them in a way that would infringe that copyright (for example, by making copies, publishing and issuing copies to the public or any other person).
- 4.3 Brief extracts of any of the material may be reproduced without the Council's permission, under the fair dealing provisions of the Copyright, Designs and Patents Act 1988 (sections 19 and 30) for the purposes of research for non-commercial purposes, private study, criticism, review and news reporting, subject to an acknowledgement of the Council as copyright owner. Wider re-use however requires our permission.
- 4.4 The Council may choose to allow re-use under licence, imposing conditions on the re-use of the information to ensure it is not used in a manner inconsistent with its copyright; and may also decide to issue a re-use fee.

#### **5. EXEMPTIONS TO RE-USE**

- 5.1 Once the Council agrees to make categories of information available for re-use, the grounds for refusing to provide any of the specific information of that type are limited to the following:
  - (a) the activity of supplying the document is one which falls outside its public task;
  - (b) the document contains content in which relevant intellectual property rights are owned by a third party; and
  - (c) the content of the document is exempt from access by virtue of the FOIA

#### **6. LICENCES AND CONDITIONS FOR RE-USE**

- 6.1 Any applicant who asks permission to re-use information for which the Council holds the copyright who has their request agreed in principle will be informed of the conditions and other licence terms. The Council will issue licences, which will include the conditions for re-use, on a case-by-case basis.

#### **7. CHARGING**

- 7.1 The Regulations state that, when allowing re-use, public authorities can make a 'reasonable return on investment'. In calculating a licence fee the Council will take into account the following:

- (a) whether Epping Forest District Council's intellectual property (ie information) has a commercial value and the appropriate level of fee which is appropriate for each individual case;
- (b) an hourly charge for staff time in making the requested information available to the applicant for re-use in accordance with the following rates depending on the seniority of the member of staff who is required to manage the request:

Head of Service	£65 per hour
Assistant Head of Service	£60 per hour
Section Head	£48 per hour
Supervisor	£37 per hour
Other Staff	£30 per hour

- (c) The cost of materials in respect of copying or printing (black & white or colour)

9 pence per double sided black and white copy

60 pence per double sided colour copy

7.2 These charges will be subject to regular reviews

## **8. INFORMATION ASSET LIST**

8.1 Where permission for re-use is granted, the Council will add the information type to an Information Asset List. The list will therefore provide a source of reference to applicants as to the type of information which has been approved for re-use. We will also link this asset list to the Council's Freedom of Information Publication Scheme.

## **9. MAKING APPLICATIONS FOR RE-USE**

9.1 An application to re-use information for which the Council holds the copyright must:

- (a) Be in writing;
- (b) State the name of the person making the request;
- (c) Give an address for correspondence;
- (d) Specify the document requested; and
- (e) State the purpose for which the document is to be re-used.

9.2 An application must be sent to the Assistant Director of Performance Management, Epping Forest District Council, Civic Offices, High Street, Epping, Essex CM16 4BZ

## **10 COMPLAINTS**

10.1 An applicant may complain to the Council about how their request for re-use has been dealt with, e.g. about any licence fee charged. This will be dealt with under the Councils Compliments and Complaints Procedure.

10.2 The complaints procedure under the regulations works in the same way as the complaints procedure under the FOIA, except that the Office for Public Sector Information (OPSI) is the ultimate authority to which to complain. An applicant can complain to OPSI only after a complaint has been considered by the Council (as the authority to which your request for re-use of information was made) and if the response to the complaint is not considered satisfactory by the person who requested the information.

10.3 Any subsequent complaint to OPSI must:

- (a) be in writing;
- (b) state the nature of the complaint;
- (c) include a copy of the written notification from the Council of its response to the complaint; and
- (d) be lodged with OPSI before the end of 28 working days commencing with the date of receipt of the Council's response.

10.4 The contact details for OPSI are:

The Standards Division  
OPSI  
Admiralty Arch  
North Side  
The Mall  
London  
SW14 2WH

## **11. UNAUTHORISED RE-USE**

11.1 The Council reserves the right to review and pursue cases of unauthorised re-use.

**Adopted by the Epping Forest District Council's Cabinet on 12 November 2006.**

## APPENDIX 4

### EPHING FOREST DISTRICT COUNCIL AERIAL CAMERA USEAGE – POLICY

#### INTRODUCTION

In March 2016 Epping Forest DC purchased two Aerial Camera Systems to be available for use by all Directorates for aerial survey purposes. On completion of the CAA Training and the publication of this policy document they will be available for service.

#### 1. POLICY STATEMENT

- 1.1 Epping Forest DC has two Aerial Camera Systems available for use by all Directorates for aerial survey purposes.
- 1.2 The systems are known as Remotely Piloted Air Systems (RPAS) (there are a number of names for these systems including Unmanned Aerial Vehicles (UAV) and Drones). The Council systems currently consist of the DJI Phantom 3 with associated software and are referred to as 'the RPAS' in this policy.
- 1.3 The RPAS will be insured for use through the Councils Insurers under out Public Liability Insurance, and this certificate will be available on demand.
- 1.4 The RPAS will be authorised for use under the Civil Aviation Authority (CAA) Permit for Aerial Work (PFAW) and only by persons trained as detailed in para 1.5 below.
- 1.5 The GIS Section is responsible for the storage, use and maintenance of the RPAS. The GIS section will have a number of operators trained in the use of the RPAS and the associated software. It is the responsibility of the Senior Business Analyst (Neighbourhoods & Governance, GIS & Gazetteer) to ensure that the training of operators and the operation of the systems are in accordance with current legislation and Industry guidelines as at para 1.4. A record of the training, CAA authorisation and maintenance of the equipment shall be kept by the GIS section.
- 1.6 It is the responsibility of the Directorate end user of the imaging gathered to ensure that the imaging is properly and lawfully used and not used for anything other than official EFDC purposes. The Data Protection Act 1998 (DPA) and Human Rights Act 1998 (HRA) are both applicable to the use of the RPAS's.
- 1.7 Any use that may come within the scope of the Regulation of Investigatory Powers Act 2000 (RIPA) must be discussed prior to the flight with the Councils RIPA Officer, and if required the necessary authorisation **must** be obtained in writing **before** the flight takes place.
- 1.8 Use of the RPAS will be controlled by the GIS Section via an electronic booking system. It is anticipated that most tasking's will be scheduled in advance but no notice tasks will occur, for example with Planning Enforcement or Land Drainage. These will be actioned as *soon as*

*reasonably practicable within 24 hours of the request, and will be retrospectively tasked on the booking system.*

- 1.9 Should a dispute arise over the priority of a use this will be resolved at the lowest level where possible. If a dispute cannot be resolved it will be decided by the Director(s) of the Directorate(s) involved.
- 1.10 The tasking will include the time, place, estimate duration, and reason for the task. There must also be a justification for the tasking under the relevant legislation. The Senior Business Analyst (Neighbourhoods & Governance, GIS & Gazetteer) or their nominee will authorise each task. In the event that more information is required the request will be returned to the originator. In the event of disputes over the justification and legality of a task this shall be referred to the Legal Section for guidance and decision if necessary. A record shall be maintained of these decisions by the Legal Section.
- 1.11 The GIS Section will keep a register of all use of each RPAS with the information included in para 1.10. Each user should also record their uses on the register held by each Directorate.

## **POLICY BACKGROUND**

- 1.12 The Council's Cabinet of 11 January 2016 authorised the purchase of 2 RPAS for the purposes of Aerial Survey for use by all Directorates. The minutes of this decisions are available on the intranet site at:  
<http://rds.eppingforestdc.gov.uk/documents/s66986/C-063%20Aerial%20Camera%20Rpt.pdf>
- 1.13 The policy has been developed in light of the HRA, RIPA and the DPA. The policy also follows the guidelines under the CAA regulations and PFAW.
- 1.14 This policy may be amended or revised at any time. Users will be notified of policy changes via email on a periodic basis, in addition to continuous posting on the Councils intranet. Fundamental changes to the policy will require a full reissue of the policy.

## **2. WHY USERS AND MANAGERS MUST FOLLOW THIS POLICY**

- 2.1 RPAS's are a growing part of modern life and their use has not been without controversy. So as to avoid reputational damage to the Council by their misuse and misuse of the images gathered this policy is designed to ensure that a chain of evidence and governance is in place for all uses of the system which can be internally and independently audited should the need arise.
- 2.2 This policy lays out the priorities for use and the mechanisms for resolving disputes over priority allocation issues.

## **3. USER ROLES AND RESPONSIBILITIES**

- 3.1 These are laid out as para 1.5 to 1.11 above.

#### 4. FURTHER INFORMATION

- 4.1 is available for Jerry Godden (Planning Enforcement Manger) x 4498 or Rob Purse Senior Business Analyst (Neighbourhoods and Governance, GIS & Gazetteer) x 4263.

#### 5. APPENDIX 1 DOCUMENT HISTORY

Revision Date	Revised by	Authorised by	Details of change(s)

### APPENDIX 5

#### EPHING FOREST DISTRICT COUNCIL POLICY FOR BODY WORN CAMERAS

Body Worn cameras

Background

This policy provides users and supervisors with the guidance to ensure that the use of the body worn cameras complies with the relevant legislations and that the data produced is retained and disposed of correctly. All staff who are to use this equipment must read and confirm that they understand this policy by signing the declaration in Annex 1.

Purpose of equipment

The use of Body-worn CCTV can provide a number of benefits which include a deterrent to acts of aggression or verbal and physical abuse toward Officers, in addition to providing evidence to support internal or other investigations. The equipment provides additional corroboration and protection without restricting an officer's action or movements. It can be used to record incidents and location providing a digital video image which can then be used in court proceedings. Additionally, it provides protection for the officers as it is a visible deterrent, making a clear statement that their actions will be recorded, and records the actions of the officer, thereby reducing the scope for false allegations. These issues are particularly relevant to officers required to work alone and in isolated areas.

Details of equipment

The Body Worn camera is an all in one, weatherproof, full high definition video recorder with articulated camera and integrated evidence management software. It consists of a body mounted camera, and because of the mounting, the equipment provider has said that it is unlikely that the camera can be ripped off. By turning the camera around, it can also be used in-car, for handheld inspections and table top for interviews.

Footage is saved on to an SD card which is removable. The SD card can only be used within the DEMS (digital evidence management system) software to be able to view the footage. You can only playback footage, and cannot delete footage on the camera itself, which is a contingency as otherwise users could lose what they record. The system must be maintained correctly as once it is deleted the data cannot be restored. Once footage is uploaded into DEMS there is a full audit trail of everything that happens on the system.

The DEMS is integrated with the RS3-SX camera to such an extent that recordings can be uploaded and managed with no user input other than simply plugging it in. RS-DEMS has been used for over five years by many Police forces and security organisations. It is a fully networked solution that provides file fingerprinting, a full audit trail, CD/DVD creation, full search and comprehensive access control. Evidence managed by RS-DEMS is routinely used in court and Reveal Media is continually extending its capabilities.

Legislation and Statutory Guidance

### **Data Protection Act 2018**

The **Data Protection Act 2018** is the UK's implementation of the General **Data Protection** Regulation (GDPR). Everyone responsible for using personal **data** has to follow strict rules called '**data protection** principles'. They must make sure the information is: used fairly, lawfully and transparently. This legislation regulates the processing of 'personal data' or 'sensitive personal data' whether processed on computer, CCTV, still camera or any other media. Any recorded image that is aimed at or may identify a particular person is described as 'personal data' and covered by this Act and will include images and audio captured using Body worn equipment. The use of Body-worn CCTV in this guidance is 'overt use' meaning that equipment is not to be worn or used in a hidden or covert manner.

### **Freedom of Information Act 2000**

This Act grants a general right of access to information held by public bodies, which is not personal data. Information released under FOI can include statistical and other non-personal information.

### **Human Rights Act 1998**

Article 6 provides for the right to a fair trial. All images captured through the use of a Body-worn device have the potential for use in court proceedings and must be safeguarded by an audit trail in the same way as any other evidence. Article 8 of the Human Rights Act 1998 concerns the right for private and family life, home and correspondence. Recordings of persons in a public place are only public for those present at the time and can still be regarded as potentially private. Any recorded conversation between members of the public should always be considered private and users of Body-worn equipment should not record beyond what is necessary when recording a confrontational situation.

The Council will further ensure that the use of Body-worn CCTV is reiterated by Officers wearing it in a prominent position (normally on their chest) and that its forward-facing display is visible to anyone being recorded. Additionally, Officers will wear identification that it is a CCTV device and make a verbal announcement prior to commencement of any recording.

### **Protection of Freedoms Act 2012**

Part 2 creates new regulation for, and instructs the Secretary of State to prepare a code of practice towards, closed-circuit television and automatic number plate recognition. Chapter 1 gives the full regulatory legislation of CCTV and other surveillance camera technology which relates to a Code of Practice and interpretations.

### **Home Office Surveillance Camera Code of Practice**

The integrity of any video data recorded will be considered in accordance with this Statutory Guidance. The Home Office is the regulator for this guidance with regard to use of Body-worn CCTV equipment. This guidance is centred around “**12 Guiding**

**Principles”** which Epping Forest District Council will adopt and adhere to at all times.

### **Information Commissioners Code of Practice**

The Information Commissioners Code of Practice is the Statutory Guidance issued that runs in conjunction with the Surveillance Code of Practice issued with regard to use of Body-worn CCTV equipment.

Guidance and responsibilities

#### Policy

- All officers must be fully briefed on the care and operation of equipment.
- All officers must understand, sign and adhere to the User Policy.

#### Roles and responsibility for security

- Overall responsibility for security and authorisation of operating officers lies with the Public Health Protection Leader Office – known as Principal Authorised Officer.
- The security and integrity of all digital video files recorded will be the responsibility of the operating officer and Authorised Officer.

#### Training

All Officers will receive full training in the use of Body-worn CCTV. This training will include practical use of equipment, operational guidance and best practice, when to commence and cease recording and the legal implications of using such equipment.

#### Recordings

Body Worn camera systems are likely to be more intrusive than the more “**normal**” CCTV style systems because of its mobility. It is therefore important to be able to justify its use and ensure that it is proportionate and necessary. Recording should not take place in more sensitive areas such as private dwellings, schools, banks or care homes etc.

There may be occasions where visual or audio recording is more intrusive than the other, for example visual recording will be more intrusive when dealing with somebody in a state of undress. With the movability of the camera end it is possible in circumstances such as this to turn the camera away but still record audio.

### Systems

- Systems are managed in line with the **Council's** Corporate Information Security.
- The software and devices are connected to a networked PC. This ensures the PC remains up to date and secure including Anti-Virus and End Point Security. This option was preferred over a standalone PC as this would require specific maintenance, and a PC with password controlled access may create a risk in itself. The PC is of a higher specification in order to effectively run the software.
- The software requires a username and login to be accessed providing another layer of security.
- Each video has the date and time stamped on every frame, a tamper proof digital fingerprint, and encryption which prevents the video being visible on unauthorised computers.
- The Supplier provides software updates which are authorised and completed by ICT Service Desk.
- The facility to burn files to DVD for court purposes in line with the Removable Media policy is subject to written authorisation by a senior manager (see Annex 3) and the DVD is to be kept in a secure evidence cupboard or passed to Legal Services
- **Data can only be written to disc in conjunction with the** Council's ICT Service Desk upon auditable request.

### Devices

- The devices are issued to named officers. Public Health and Protection hold details of the systems and their serial numbers signed for by Operating Officers.
- Operating Officers are responsible for the devices held by them and they, and the SD Cards may not be re-allocated to another officer without them being signed for and countersigned by the Principal Authorised Officer. No officer may be allocated the unit unless they have signed the agreement in Annex 1.
- Devices must be returned and downloaded prior to terminating duty. Supervisors/Authorised Officers will ensure that this has been complied with. This will ensure that all recordings are stored on the computer, the device memory is empty and the device is ready (i.e. empty) to be taken out and/or assigned to the next user.
- Prior to its next use the data and time stamp should be checked to ensure it is accurate.
- When images with evidential value are recorded the officer downloading these onto the computer should mark these appropriately, to prevent accidental deletion.
- The equipment displays the footage it is recording on its screen and is thus clear that it is a camera. The Operating Officers are however instructed to notify the subject that their conversation is being recorded.

#### Retention of data

- When the user uploads to DEMS they must be marked as either **evidential** or **non-evidential**.
- Anything non-evidential sits under the Data Protection Act, and must be deleted after 31 days.
- There are two ways to run the DEMS system with regards to data protection, a manual or automated system.
  - Manual System – DEMS will tell you how many recordings you have in your system over the Data Protection limit (usually 31 days) can be reviewed and deleted or change to evidential if the status has changed. The Operating Officers must seek permission from the Principal Authorised. Form attached at Annex 2.
  - Automated – The Authorised officers set the data protection limit (general advice is 31 days) and then anything that has been flagged as non-evidential that gets to 32 days over will be deleted automatically.
- Images of non-evidential important will be kept for a period of 31 days in keeping with existing guidelines for the storage of video images.
- Any images requested by the police as part of their investigation will be burnt to disc, labelled as an official exhibit and handed to them. Once in their possession the disc will fall under the police policy and guidelines for Data Protection. Details of this process and any relevant information i.e. PC name or collar number, date, time etc. will be logged so there is a full audit trail.
- Those images which have evidential importance and may be required for court proceedings will not be destroyed until after 6 weeks from the date of prosecution and confirmation that no appeal has been lodged. The Operating Officer recording the data will be responsible for ensuring the data is destroyed.

#### Disposal of data and devices

- All storage media should be disposed securely in line with ICT procedures. This includes flash/SD cards (as used in digital cameras) and any other device on which data can be stored. Services must contact the ICT Service desk who will complete this with an assured media destruction company.

#### Data Subject Requests

- Individuals whose information is recorded have a right to be provided with that information, or if they consent to it, view that information. Information must be provided within 40 calendar days of receiving the request, however our retention period is 31 days for non-evidential footage so it would need to be prior to any non-evidential footage being deleted.
- If a request is received then the Principle Authorised Officer will need to be notified and a decision made on how to provide the individual with copies of the information taking into account any third party information that may need obscuring.

Annex 1 – Authority to Assign Body Worn Camera to an Operating Officer

**The Body Worn Camera Serial No** .....

**Previously issued to** .....

**Is re-assigned to** .....

**Date** .....

Declaration of adhering to the Body Worn Camera policy by New Operating Officer

- I have read and understood this policy, and am confident that the information and training provided will enable me to adhere to this
- I fully understand my responsibility of a user of this equipment and software, and will ensure that I follow the relevant legislation when using this.

<p><b>User</b> <b>Officer</b> ..... <b>Job Title</b> ..... <b>Date</b> .....</p>
--

**Re-assignment agreed by Principal Authorising Officer**

<p><b>Supervisor/authorising officer</b> <b>Officer</b> ..... <b>Job Title</b> ..... <b>Date</b> .....</p>
--

Annex 2 – Authority to change the status of Non-Evidential to Evidential data.

The status of the following data should be changed from non-evidential to Evidential

Date of footage.....

Title .....

Recorded by .....

Reason for change .....

.....

.....

.....

.....

.....

<b>User</b>
<b>Officer</b> ..... <b>Job Title</b>
.....
<b>Date</b> .....

Agreed/Refused\*

<b>Supervisor/authorising officer</b>
<b>Officer</b> ..... <b>Job Title</b>
.....
<b>Date</b> .....

Annex 3 – Authority to Burn Data to DVD

Authorisation is required to burn the following data to disc

Date of footage.....

Title .....

.....

Recorded by .....

Reason for request .....

.....

.....

<b>User Officer</b> .....
<b>Job Title</b> .....
<b>Date</b> .....

Comment .....

.....

<b>Supervisor/authorising officer Officer</b> .....
<b>Job Title</b> .....
<b>Date</b> .....