

CCTV Recording Compliance Guide

October 2001

Incorporates

**Section 1
Data Protection Act 1998 Summary
Interpretation**

**Section 2
Elements of Good Practice**

**Section 3
Site Specific Code of Practice**

IMPORTANT

This Compliance Guide is designed to assist operators and managers of CCTV recording systems in operating their CCTV systems in an effective and legal manner.

The guide incorporates a reasonable interpretation of The Data Protection Act and Human Rights Act as it affects CCTV users, it also contains a section detailing recommended Elements of Good Practice and a Model Code of Practice that can be made site specific. **Those preparing this guide have done so in good faith and can not accept any responsibility for making an incorrect interpretation. It remains the responsibility of the system owner/manager to obtain a copy of the relevant Act and other Standards and make his/her own interpretation and put the matter into practice.**

It is in essence a guide for the layperson who is responsible for the management of a CCTV recording system. This is an interpretation of the Data Protection Act and Human Rights legislation together with recommendations by Police, Home Office and British Standard 7958:1999, in a practical and pragmatic manner.

Should the reader wish to develop a more in depth knowledge of the subject it is recommended that he/she obtain copies of the relevant Acts and Standards.

Data Protection Act 1998 Summary.

Section 1

1:01 The Act.

The Data Protection Act 1998 relates to data processing of all types. The definition of data under the new Act is "Information which is being processed by equipment operating automatically in response to instructions; or is recorded with the intention that it should be processed".

Having regard for these definitions, it will be recognised that the use of CCTV for surveillance purposes is encompassed in the new Data Protection Act .

Data in the case of CCTV recordings is in the form of recorded images of individuals that can be identified from these images.

The Act states that system owners must formally notify the Office of The Information Commissioner that they are processing data unless they have already done so for other purposes covered by the Act.

You must notify the Data Protection Registrar by the 24th of October 2001.

To notify the Office of the Information Commission you may either do so on the DPA web-site www.dataprotection.gov.uk or telephone 01625 545700.

1:02 Data Protection Principles.

The Data Protection Act has eight principles that data should be processed in accordance with. The principals are as follows:

1. "Personal data should be processed fairly and lawfully".
2. "Personal data shall be obtained for one or more specified purposes, and shall not be further processed in any manner incompatible with those purposes".
3. "Personal data should be adequate, relevant and not excessive in relation to the purposes for which they are being processed".
4. "Personal data should be accurate and, where necessary, kept up to date".
5. "Personal data processed for any purpose or purposes shall not be kept for any longer than is necessary for that purpose or those purposes".
6. "Personal data shall be processed on accordance with the rights of data subjects under this Act".
7. "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data".
8. Personal data shall not be transferred to country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedom of data subjects in relation to the processing of personal data".

How does this translate to the way we operate CCTV systems? A system should be evaluated using the following criteria.

1:03 Evaluation Criteria.

1. Objectives of the scheme in question.
2. Fairness of the scheme.
3. Confidentiality of images recorded and handled.
4. The rights of individuals of whom data is being collected.

These four points are developed as follows:

1:03:01 Objectives / Purposes of the Scheme (Second Data Protection Principle).

Operators must have access to a clear documented statement of the objectives of the scheme. This document must also include the responsibilities of those involved in operating and managing the system.

The purpose for operating the scheme should be lawful.

1:03:02 Fairness (First Data Protection Principle).

Individuals should be made aware that they are entering an area where CCTV recordings are active. This is normally achieved by the use of signs. Signage should display the following information:

- * A warning that CCTV recording is taking place.
- * The purpose of the scheme.
- * The operators of the scheme.
- * Contact details for the operators of the scheme.

If the correct signage is not in place the scheme will be considered covert. Covert recordings can only be made under the following circumstances:

- * If you have assessed that informing individuals that recording was taking place would prejudice your objectives.
- * You have reasonable cause to suspect specific criminal activity.
- * That the covert processing is only carried out for a limited, and reasonable period of time and relates to specific criminal activity.

If you decide in principle to adopt covert recording, you would be advised to have a clear documented procedure, which sets out how you determine whether the use of covert recording is appropriate in an individual case. If you decide that covert recording is appropriate, you should document your decision and the reasons for reaching that decision.

Recommended Sign Sizes and Designs.

Whilst the DPA Code of practice makes certain suggestions as to the size of signs it makes no reference to Colour. The obvious choice if high impact colour would be a traffic yellow background printed in black as standard industrial warning signs. Such a choice of colour is acceptable in most industrial, commercial and government applications, however, a more subtle engraved brass or stainless steel finish would be more appropriate in certain applications. In the case of Bank ATM machines with CCTV recording an on screen statutory information sign would be ideal providing that the sign is visible before the start of any recording that takes place. There is no substitute for common sense, but as a guide:

- A3 Size for outdoor perimeter applications and multi-storey car parks.
- A4 Size for large building entrances.
- A5 Size for single leaf doors

1:03:03 Confidentiality. (Seventh Data Protection Principle).

This is one of the most important sections of the Data Protection Act 1998. It is not a very difficult concept but has far reaching effects as far as traceability, security and accountability is concerned. All the images that you record are considered confidential, this would include video prints etc.

1:03:04 Traceability.

To ensure confidentiality the Data Protection Act requires traceability of images. This implies that each image could be traced to a specific date, time, recording device, recording medium and the individual responsible for the recording. This is normally achieved by means of a written log.

1:03:05 Time and date stamping.

By inserting the time and date and the camera reference on the images it enables you to refer to a specific incident.

1:03:06 Serial numbers.

The recording medium can be made traceable by using serially numbered cassettes.

Cassettes should be dedicated to specific recording devices and should not be interchanged between machines. Tapes should not only be traceable through their lifetime, but also through their individual uses.

1:03:07 Security.

We have already mentioned the fact that these images are confidential. This creates the need for security of both the recording media, the images on this media and the recording devices.

Tapes should be stored in lockable cabinets. This would restrict access to all unauthorised parties. It would also ensure the archiving period is maintained. Tapes should be kept in secure cabinets even in a control room situation.

Equipment should be kept in tamper proof conditions. Access to the recording equipment should be restricted to maintenance staff and operators. Access to recording equipment by maintenance engineers should be logged.

1:03:08 Erasure.

Tapes should be erased between recordings and at the end of their lives. Because the information is confidential it is important to destroy the evidence on the tapes before they are discarded. Erasure of tapes should be checked and logged.

1:03:09 Archiving (Fifth Data Protection Principle).

Information should not be stored longer than necessary. The generally accepted norm is 31 days. Images may be stored for longer periods if it can be justified, for example 90 days in the case of Bank ATM where a customer may not be made aware of a problem until a bank statement is received.

1:03:10 Quality of Images (Third and Fourth Data Protection Principles).

Images should be of such quality that the purpose of the scheme can be achieved. The equipment should be restricted to record sufficient information to achieve this purpose. Care should be taken that no unnecessary information is gathered.

1:03:11 Information Sharing (Eight Data Protection Principle).

Section 115 of the Crime and Disorder Act 1998 creates the power to share information, from the system owner / operator to the Police Authorities, Probation Committees, Local Authorities and Health Authorities. All relevant information should be documented, including the reason for information sharing.

For the avoidance of confusion it would be good practice not to issue recordings to any third parties other than the Police.

1:03:12 Evidence Recordings.

Any recordings used for evidence should be segregated from the normal tapes and kept in a secure manner. Copies of recordings may be admissible as evidence providing there is a clear audit trail to the original copy.

1:03:13 Tape Copies and Video Prints.

Any copies of recorded material should be documented and made trace-able.

1:04 Rights of the Individual (Sixth Data Protection Principle).**1:04:01 Access.**

Individuals may request a copy of any recording that exists of them, this would normally be in the form of a video recording on a VHS cassette. He/she must be made aware of their rights regarding such recordings by means of a summary of the rights of the individual and the system owner/operators.

If the owner/manager cannot comply with the request without disclosing identifiable images of third parties, the manager or a designated member of staff should determine whether the images of the third party is held under a duty of confidence. In which case the images shall be edited to disguise the identities of such parties.

If you have any doubts regarding this matter it would be prudent to err on the side of caution and arrange for third party images to be electronically masked.

Access may be denied where such an action would compromise the detection or prevention of crime, or where it may impede the apprehension or prosecution of offenders.

1:04:02 Privacy (Sixth Data Protection Principle).

IMPORTANT THIS PRINCIPLE APPLIES TO ALL SYSTEMS WHETHER OR NOT RECORDING IS TAKING PLACE

Cameras should be set to view only images that they were intended in order to achieve the objectives of the scheme. If this is not possible without viewing domestic or other areas would be reasonably considered private, the owner of these areas should be consulted.

If you have any doubts regarding this matter it would be prudent to electronically or physically obscure the view such cameras have of private areas.

Intentional voyeurism via operation of CCTV cameras is an invasion of privacy in any circumstances. Employers of CCTV operatives should consider making evidence of such unacceptable behaviour grounds for disciplinary procedure.

1:04:03 Definitions.

In order to have accurate and complete documentation to accompany your system, you need to understand some of the terms used in the Data Protection Act.

1:04:04 Data Controller.

"A person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed".

In the case of situations where CCTV is the only data being processed this individual would be the senior person within the system owners organisation who has responsibility for security policy.

1:04:05 Personal Data.

Data which relates to a living individual who can be identified:

- a) from those data, or
- b) from those data or other information which is in the possession of, or is likely to come into the possession of, the data controller.

1:04:05 Sensitive Personal Data.

Section Two of the Act 1998 separates two distinct categories of personal data, which are deemed sensitive. A full list of these categories are available in section two of the Act. The following are the main two reasons that would deem data to be considered as sensitive.

- a) The commission or alleged commission of any offences.
- b) Any proceedings for any offence committed, or alleged to have been committed, the disposal of such proceedings or the sentences of any court in such proceedings.

1:04:06 Beneficial Owner.

The owner of the system being the person or organisation that receives benefit from the operation of the system. In the event that the system is leased from a finance company the lessee would be considered to be the owner for the purposes of the DPA not the finance company.

Elements of Good Practice

2:01 Traceability and Record Keeping.

Recordings must be identified by a unique serial number indelibly marked on the cassette shell, in the case of magnetic tape.

Whatever media is adopted, the unique identity of the recording is obviously compromised if it is applied only to the outer wrapping or cover.

Recordings must be logged and traceable throughout their life within the system.

A logbook system entry must be made of tape use and recorded incidents. It must be able to demonstrate the location of any recording during its lifetime within the system and that, ultimately it has been erased before being disposed of or physically destroyed.

Always fully rewind a replacement tape and zero the machine counter before starting to record.

A routine audit should be undertaken at regular intervals to ensure that all tapes logged into the system are present. Irregular spot checks are also advisable.

Original recordings should only be found:

- a) within the recognised secure storage system.
- b) operational in the recording device.
- c) secured as evidence.

Copies of recorded information must be strictly controlled and only be made in relation to incidents the subject of investigation, or a valid subject access request. Copies must only be issued by the system manager to those directly connected with achieving the objectives of the system.

2:02 Time and Date Stamping.

The correct time and date must be overlaid on the recorded image. In the case of a simple system with one video recorder the time and date display is normally a function of this machine. A known accurate point of reference, such as the speaking clock, must be used to set the time and the BST to GMT changeovers must be routinely dealt with.

Where systems incorporate a number of recorders it is particularly important to synchronise the time and date display. A Rugby Clock system is the preferred solution. Evidence may be called for that involves recordings from a number of machines, if the time display is not synchronous between recording machines evidence could be made to appear nonsense.

The location of the camera should also be displayed within the relevant camera frame.

2:03 Recording Archive Period.

The archive period of recordings shall be no longer than is necessary to achieve the objectives of the system. The generally accepted period is 31 days although if there is reasonable cause to extend this period a longer duration of storage may be acceptable.

2:04 Magnetic Tape Life.

The generally recognised maximum number of recording passes for VHS/SVHS tape is no more than twelve. It is set at this level to reduce the possibility of tape breakage and degradation of recordings due to mishandling and poor environmental conditions.

When giving consideration to setting the maximum number of recording passes for the various types of digital cassette, it may be unnecessary to adopt the same number as for VHS. It would be good practice to contact the recording machine manufacturer for advice.

Whatever the decision, this should be made at the outset and the Start and Projected expiry dates should be indelibly noted on the body of the cassette.

2:05 Magnetic Tape Erasure.

Tapes should always be magnetically erased between recordings.

"Simply recording over old material is not satisfactory, not least because this will compromise a tape's acceptability for evidential purposes" THE HOME OFFICE PUBLICATION "CCTV LOOKING OUT FOR YOU", Nov.1994

Tapes must always be magnetically erased and spot checked for erasure before being disposed of or destroyed.

2:06 Secure Storage of Recordings.

The recordings and recording/processing equipment must only be accessible to those directly concerned with achieving the objectives of the system.

Recordings and recording/processing equipment must be either located in a formal, secure CCTV control room environment or must be secured in a lockable enclosure accessible only to authorised keyholders, a key register must be maintained.

Each recording machine must have its own dedicated and effectively segregated tape stock.

2:07 Multiple Recorder Systems.

Where systems incorporate a number of recorders, it is particularly important to dedicate tapes to specific recorders. Tapes should never be allowed to cross-over between different machines.

Always synchronise the time and date display. A Rugby Clock system is the preferred solution.

2:08 Recording Periods.

In deciding the length of recording time per tape, take into account that the shorter the recording period, the more detail you will record.

Another important factor is that if recorded evidence is produced in Court, it is probable that the member of staff responsible for the recording will be called to vouch for its veracity. If the recording period extends from one persons shift into another, you will be faced with the problem and cost of producing two members of staff. For this reason alone it is unwise to set a recording period greater than a working shift of say, 8 or 12 hours.

2:09 Recording Quality.

At the end of each recording period rewind the tape and carry out a random spot replay to ensure a reasonable quality of recording is being achieved. Without this simple check it is possible that a faulty recording machine or tape could go unnoticed for a considerable period.

2:10 Evidence Handling.

Original evidence recordings must have the recording prevention device set to "safe". They should then be segregated from operational recordings and held in a secure manner, only accessible to those directly concerned with achieving the objectives of the system.

It is preferable that the original recording should not be passed to any third party and must be sealed in a tamper apparent evidence bag, together with the original of the incident report. This should then be placed in a secure enclosure pending any requirement for it to substantiate the copy recordings.

Both original and any copy recordings must be magnetically erased and/or physically destroyed upon official closure of any investigation relative to the subject matter.

IT IS ADVISABLE NOT TO PASS ANY RECORDING TO ANY THIRD PARTY OTHER THAN THE POLICE.

Section 3

Site Specific Code of Practice

This section to be completed by the installer and/or end-user and placed in the system logbook.

3:01 Introduction.

This code of practice relates to the Closed Circuit Television System installed at

The beneficial owner of the system is _____

The owners managing agent is _____

and the system is registered with the office of the Data Protection Registrar.

The system manager is

Print Name _____ Signature _____

The designated Data Controller is _____

The Data Protection Act registration number is _____

The system is operated by the following individuals
An extension to this list is appended (tick if applicable)

	Name	Job Title	Signature
1.	_____	_____	_____
2.	_____	_____	_____
3.	_____	_____	_____
4.	_____	_____	_____

The above signatories will sign to indicate that they have read and understand this Code of Practice and the preceding sections: 1. Data Protection Act 1998 Summary and 2. Elements of Good Practice.

3:02 Objectives.

Tick

- _____ To assist in the detection of crime.
- _____ To provide evidence of crime.
- _____ To deter those having criminal intent.
- _____ To give confidence to Staff and Visitors that they are in a secure environment.
- _____ To provide management information relating to Health and Safety matters.
- _____ To provide information relating to vehicle traffic management.
- _____ To provide information relating to the good management of the premises.

3:03 System.

The system comprises the primary items of equipment listed below and as per the System Diagram which would be supplied by your system installer and filed in the CCTV logbook, Volume 1 Section 4.

Qty.

- _____ Fixed position cameras
- _____ Full feature Pan, Tilt and Zoom cameras
- _____ Monitors
- _____ Multiplexers
- _____ Video recorders designated record only
- _____ Video recorders designated play back only
- _____ Photographic video printer
- _____ Magnetic tape eraser
- _____ Public information signs "CCTV Recording Operational in this area"
- _____ Recording tapes
- _____ Additional items _____

3:04 Operations Manual.

An operations manual relating to the specific items of equipment has been compiled by the installer of the system and is held

_____ (state location)

It is the responsibility of the system manager to ensure that staff are aware of the function and capable of operating the various items and equipment within the system.

3:05 General Principles.

3:05:01 The principles detailed in **Section 1, Data Protection Act Summary** and **Section 2, Elements of Good Practice** will be observed in the operation and management of the system.

3:05:02 A CCTV Logbook will be maintained incorporating the following sections:

	Section	Tick	
Volume 1	Section 1	_____	Tape log
"	Section 2	_____	Incident report
"	Section 3	_____	This Site Specific Code of Practice
"	Section 4	_____	System Diagram and operating manual
"	Section 5	_____	Right of subject access forms
Volume 2	Section 1	_____	Operator duty log
"	Section 2	_____	Visitor log
"	Section 3	_____	Repairs and maintenance
"	Section 4	_____	Video print log
			Other _____

3:06 Recording Management.

3:06:01 Tapes will be used for a maximum of _____ (enter number) recordings, each before being subjected to a final magnetic erasure and disposal by

Magnetic erasure

Magnetic erasure and mechanical destruction

Each use of a recording tape will be logged in **Volume 1 Section 1** of the CCTV logbook. Each recorder will have a dedicated section, each tape will have a dedicated page.

3:06:02 The recording system is

Tick
 _____ VHS
 _____ SVHS
 _____ DIGITAL

The cassettes are individually identifiable by unique serial number.

- 3:06:03 Tapes will be magnetically erased between recordings, it is not permitted to record over old material.
- 3:06:04 The recording machine's tape counter will be zeroed before each recording is commenced.
- 3:06:05 The time and date display as appearing on screen will be checked as correct before each recording is commenced.
- 3:06:06 At the end of each recording session the tape will be fully rewound. During the rewind a random view will take place to ensure that both the recording machine and tape are functioning correctly.
- 3:06:07 Each tape will be dedicated to a specific recording machine and will be held in a storage position bearing the same reference number as the machine.
- 3:06:08 The recording machine will be set at _____ (enter hours) hr. recording mode.
- 3:06:09 Tapes will be changed daily at _____ (state time).
- 3:06:10 The tape archive comprises of _____ (quantity) tapes and the operational tape stock will be audited every _____ (state period e.g.12 months)
 Any serial numbers found to be missing without explanation will be noted MISSING-LAST RECORDED USE ???/??/?? In **Volume 1 Section 1** (tape log) of the CCTV logbook.

3:07 Incident Reporting.

- 3:07:01 An incident report, **Volume 1 Section 2** of the CCTV logbook, will be completed for each incident requiring investigation.
- 3:07:02 Assuming that facilities exist for duplication, a copy tape will be made and issued to the Police.
 together with a copy of the incident report. The original of the incident report will be held in

(the logbook or in the designated secure lockable enclosure)

3:08 Video Prints.

- 3:08:01 Video prints may only be issued by the system manager or his deputy.
- 3:08:02 The issue and control of video prints will be recorded in **Volume 2 Section 4** (video print log) of the logbook, a label adhering to the back of each print and a carbon control copy held in the logbook. Any data subject requests should be documented on right of access request forms.
- 3:08:03 It is the responsibility of the system manager to ensure that video prints are recovered at the completion of an investigation and destroyed by

(state method)

The system manager will indicate that destruction has taken place by placing a cross on the control copy together with his signature.

3:09 System Maintenance.

- 3:09:01 The system maintenance is contracted with _____ (contractors name)
 of _____ (contractors address)
 Service is available

(state times, days of the week) and a response time of _____ (hours) is agreed, the contractor must provide an engineer on site within this time and the reported fault must, if possible, be fixed within _____ (hours). If a final fix is not achieved within this period and a further site visit is required the final fix must be completed within _____ (hours).

3:09:02 Video recorders will be refurbished as per manufacturers recommendations, at intervals not exceeding _____ (hours).
Service replacement units will be provided if a machine is removed from site.

3:09:03 Any fault call out or routine maintenance visit will be reported in **Volume 2 Section 3** (repairs and maintenance) of the logbook.

3:10 Visitors.

3:10:01 Visitors to site having any connection with the CCTV system, i.e. Police, Service Engineers, Members of the Public, in connection with a Subject Access request, previously agreed with the system manager or

_____ (state whom)

must log on and off site in **Section 2 Volume 2** (visitor log) of the CCTV logbook.