

What to do first...

- 1 Print off the following copies of the documents on this CD.
 - 1 x Site Details Form.
 - 1 x CCTV Cassette Recording Log per cassette used.
 - 1 x CCTV Cassette Stock Check & Disposal Log.
 - 1 x Code of Practice Checklist.

You may not need the following forms immediately but it may be useful to keep copies for easy access in your CCTV Log Book folder.

Subject Access Request Form & Leaflet.
Fee Sheet.
Incident Log.
Visitors / Maintenance Log.

- 2 Complete the "Site Details Form" & file at the front of your "CCTV Log Book folder".
- 3 Register your CCTV system with the Information Commissioner (details below). By registering your CCTV system & following the enclosed guidelines your recorded images will comply with the Data Protection Act. Failure to comply may affect the police's ability to use your recorded CCTV images & may hamper the prosecution of offenders.

Information Commissioner
Wycliffe House, Water Lane, Wilmslow,
Cheshire SK9 5AF

Tel: 01625 545700 Fax: 01625 524510
E-mail: data@dataprotection.gov.uk
Website: www.dpr.gov.uk

Cost: £35.00 (no vat applicable (as of August 2002)).

- 4 You will need 1 CCTV Cassette Recording Log for each cassette used in your system. Each cassette requires a unique serial numbered identification. These can be purchased as part of our CCTV Cassette Pack. (Order Code: LEA102). Label each cassette with one of unique serial numbered labels & each recording log with a matching serial numbered label.

Complete the general information on the Recording Log such as site address, cassette type, machine location etc.

- 5 Your camera control equipment, recording equipment & cassettes should be stored in a secure location where only authorised personnel can access the equipment. This may be in a locked room, cupboard or lockable cabinets designed especially for this purpose. (Please see our "CCTV World" catalogue for more details on these cabinets).
- 6 It is recommended that each CCTV Cassette is used a maximum of 12 times & then disposed of. It is also recommended that a stock check is carried out at frequent intervals to ensure that no footage has gone missing, been damaged or been taken without authorisation. The management of your cassettes can be recorded in the "CCTV Cassette Stock Check & Disposal Log". Cassettes should be erased before disposal. This can be done by recording a blank picture on the cassette on a normal VCR.
- 7 At any time, a person who believes that they have been recorded by one of your system's CCTV cameras may request to view the images. Under the Data Protection Act you are obliged to allow them to see those images but you can levy a charge to cover any costs involved in supplying this information.
For this purpose, there is a "Subject Access Request Form" & Fee Sheet included. Whilst the recorded images are in the 'subjects' possession, they are not your responsibility. You may choose to supply a cassette copy of those images only & retain the original cassette in your possession.
- 8 When & if an incident occurs, the details should be itemised in writing using the "Incident Log". This log should be cross referenced with the cassette on which the incident was recorded using the unique serial number on the cassette's label. If it necessary for the cassette recording to be taken off the premises to be used as evidence, it should be kept in a sealed Video Evidence Bag between viewings. This is supplied in the CCTV Cassette Pack (Order Code LEA102).

- ⑨ If a member of the general public or a police officer wished to view data and images on the CCTV system, it is wise to note the details of their visits in writing using the "Visitors & Maintenance Log" enclosed.
- ⑩ You will need to use the same log if any maintenance visits or emergency call-outs are made on the system. Your log should include any work carried out on the system.
- ⑪ Signs - with only a few exceptions (listed in our Code of Practice summary), it is necessary to make members of the general public including visitors and staff to your premises aware when they are entering into a CCTV recording zone. This can easily be done using appropriate signage. By warning a subject that the area they are about to enter is being recorded, by passing the sign and entering the area they have indirectly agreed to be recorded.

The appropriate size of a sign will depend on the environment. For example, a C5 window sticker might be suitable at eye level on a glass door entering a shop, a couple of A4 signs might be suitable on a shop floor or in a restaurant or an A3 sign might be suitable mounted at the barrier of a car park where drivers entering the area know that they are being recorded.

- ⑫ On an annually basis, you will need to examine your CCTV scheme to make sure it is working inside the guidelines and for the purposes that you have registered it for. We have enclosed a Checklist on the disk and suggest that this is completed at least once a year preferably just before you re-register your system with the Information Commissioner.

Remember - the above is a simple to follow list, to better understand why these guidelines should be followed, read our CCTV Code of Practice Summary on the enclosed disk.

CCTV SITE INFORMATION

General information on the CCTV system to be completed by the system owner/manager.

- The CCTV system described in this CCTV log book is installed at the following premises:

Address:	
Postcode:	Telephone:
The owner of this system is:	
Name or Company name:	
This system was registered with the Data Protection Registrar on: / /	

(To register your new system, go to: www.dpr.gov.uk)

- Key staff managing and using the system are as follows:

	Name	Job Title
System Manager:		
Data Manager:		
Operator 1:		
Operator 2:		
Others:		

(Logs of those operators on duty can be found in the Duty Log of this guide.)

- External contractors engaged in the installation and maintenance of this system, can be contacted as follows:

Company:	
Address:	
Postcode:	Telephone:
Contact name:	

- The purpose of this CCTV system is to:

Please tick appropriate box....

- assist in detecting crime carried out by visitors to the premises.
- assist in recording violent actions carried out by visitors to the premises.
- deter those with criminal intent, staff or visitors.
- reassure staff and visitors to the premises that this is a safe environment.
- assist in the monitoring of staff for health & safety and training purposes.
- assist in market research.
- provide evidence of crimes carried out against the owner of this system.

● The system comprises the following equipment:

Cameras	Quantity	Locations / Serial Number(s)
External fixed overt B&W Cameras	
External fixed overt Colour Cameras	
Internal fixed overt B&W Cameras	
Internal fixed overt Colour Cameras	
External fixed covert B&W Cameras	
External fixed covert Colour Cameras	
Internal fixed covert B&W Cameras	
Internal fixed covert Colour Cameras	
External PTZ B&W Cameras	
External PTZ Colour Cameras	
Internal PTZ B&W Cameras	
Internal PTZ Colour Cameras	

Monitors		Quantity	Locations / Serial Number(s)
B&W	9" Monitor	
	12" Monitor	
	15" Monitor	
	17" Monitor	
	20" Monitor	
	Other B&W Monitors...	
Colour	14" Monitor	
	21" Monitor	
	Other Colour Monitors	

Control Equipment		Quantity	Locations / Serial Number(s)
*Multiplexer units		
*Quadsplitters		
*Switchers		

Recording Equipment		Quantity	Locations / Serial Number(s)
*Standard VCR		
*Timelapse VCR,	Type eg. 24hr
*Cassettes	Type eg. E180
	Type eg. E240

Other Equipment	Quantity	Locations / Serial Number(s)
.....
.....
.....
.....
.....
.....
.....

(* The items marked with an asterisk must be kept in a locked area or storage cabinet to prevent unauthorised access to data. This data should only be accessed by personnel stated at the front of this form.)

● Instruction and operating manuals supplied for this CCTV system are stored in the following 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 of equipment within the system.

● This CCTV logbook contains the following reports and logs on this CCTV system:

- ① CCTV Cassette ID Log,
- ② Incident Log,
- ③ Cassette Stock Check & Disposal Log,
- ④ Subject Access Request Forms & Fee Sheets,
- ⑤ Visitors/Maintenance Log,
- ⑥ Annual Checklist,
- ⑦ Copy of the Code of Practice Summary.
- Other...

(Please tick if included)

Recording Information.

● Full information regarding each cassette, its usage, access to it and its disposal will be recorded in the Cassette ID and Cassette Stock & Disposal Logs relating to this system (enclosed).

A QUICK CHECKLIST

Date: / /

Completed By:

SITE ADDRESS

Company/Branch Name:

Address:

Postcode:

Telephone:

Please check that the following points have been verified in relation to the CCTV system on the above site.	Please tick below when checked	Checked by: (name)	Date of Check	To be reviewed on (date)
<i>Notification of this CCTV system has been supplied to the Information Commissioner for the next 12 months.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>The system has been registered and is due for renewal on: / /</i>	<input type="checkbox"/>	/...../...../...../.....
<i>The quality of images recorded on the system are sufficient quality for the police to use them to investigate a crime.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>CCTV cameras at the site are positioned to avoid capturing images of anyone not actually attempting to visit the premises.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>Signs showing those responsible for the CCTV system and how to contact them are displayed on the premises where it is not obvious who is responsible for the system.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>All recorded data is securely stored on the premises with permitted access to a limited number of staff.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>Recordings are only held for sufficient time enough for an incident to come to light & to be investigated.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>Recordings will be made available to the police etc. for the purpose of the prevention and detection of crime.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>The system controller is aware that requests to view recordings may be received by individuals who believe they have been captured on the CCTV system and a set procedure is in place to deal with such a request.</i>	<input type="checkbox"/>	/...../...../...../.....
<i>The CCTV equipment at the above site is regularly serviced and checked to ensure accurate data is captured.</i>	<input type="checkbox"/>	/...../...../...../.....

CCTV CASSETTE RECORDING LOG

SITE ADDRESS

Name _____

Address _____

Postcode _____

Telephone No. _____

CCTV Cassette I.D. _____

Cassette Type - eg. E180, VHS _____

VCR Ref / Location _____

USAGE LOG

Use	Recording Started At & By:				VCR Check (*A)	Rec. Mode Used eg. 72hr	Recording Ended At & By:				Record Check (*B)
	Date	Time	Sign	Print			Date	Time	Sign	Print	
1/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
2/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
3/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
4/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
5/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
6/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
7/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
8/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
9/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
10/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
11/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>
12/...../.....				<input type="checkbox"/>/...../.....					<input type="checkbox"/>

MAXIMUM RECOMMENDED NUMBER OF RECORDINGS

INCIDENT REPORT

Date: / /

Time:

Incident Report Log No.:

(*A) Check VCR time & date is accurate and that the VCR counter is at zero.

(*B) Check that the VCR has recorded images and that it is rewound.

The maximum recommended number of uses for this cassette has been reached. Please dispose of carefully.

Cassette Disposal Date:

SUBJECT ACCESS REQUEST FORM

REQUESTED BY

Name:

Representative of:

Badge no: (if applicable)

Address:

Postcode:

Contact tel no:

REASON FOR REQUEST

Crime no. (If applicable)

DECISION

(Please tick appropriate box)

Accepted

Rejected

Reason given:

RELEASE OF CASSETTE

Copy

Original

Cassette I.D.

Released by: (name) Released on: (date)/...../.....

IMPORTANT TO BE SIGNED BY THE PERSON THAT THE CASSETTE IS RELEASED TO.

I accept full responsibility for the care of this cassette and any access given to a third party.

Signed: Printed: Date:/...../.....

RETURN OF CASSETTE

Date of return:

Returned by:

Accepted by:

Condition of cassette:

Good

Fair

Poor

Cassette returned to system:

Yes

No

Location:

Cassette in poor condition, method of disposal:

SUBJECT ACCESS LEAFLET

Company Name:
Site Address:

- At the above premises, CCTV is used for the monitoring and collection of sound and visual images for the purpose of maintaining the security of the premises & for preventing crime & investigating it.

The subjects that this system is likely to record in its day-to-day operation include:-

Please tick any box that is appropriate.

- Staff.
- Customers.
- Contractors.
- Members of the general public.
- Offenders / suspected offenders.
- Those entering the vicinity of the CCTV recording zone.

- The system is used to record the following data:

Please tick any box that is appropriate.

- Criminal behaviour.
- Provision of goods & services.
- Staff training & conduct.
- Sound or visual images of visitors to premises.
- Market research findings.

- Data collected on this system may at times be viewed by members of the following groups:

Please tick any box that is appropriate.

- Any subject who has had data captured about them.
- Designated employees & the Data Controller.
- Police forces or security organisations.
- Suppliers / providers of a good or service.
- A professional advisor.
- A person making a complaint.

- If you have any further questions on this CCTV system & how our data is protected, you may contact...

on tel:

SUBJECT ACCESS - FEE SHEET

Request Approved For: (name)

Date: / /

Fee Applicable £

Paid By: Cash | Cheque | Credit Card | Other, please state



SUBJECT ACCESS - FEE SHEET

Request Approved For: (name)

Date: / /

Fee Applicable £

Paid By: Cash | Cheque | Credit Card | Other, please state



SUBJECT ACCESS - FEE SHEET

Request Approved For: (name)

Date: / /

Fee Applicable £

Paid By: Cash | Cheque | Credit Card | Other, please state



SUBJECT ACCESS - FEE SHEET

Request Approved For: (name)

Date: / /

Fee Applicable £

Paid By: Cash | Cheque | Credit Card | Other, please state

SITE INCIDENT LOG

CCTV Cassette I.D.

Incident No.

Description of Incident

Cassette Format
eg. E180 VHS
.....

Rec. Mode
.....

Incident Date
..... / /

Incident Time
.....

VCR Counter No.
.....

Described By:	Date: / /
Signed:	

RELEASE OF RECORDING

Date: / /

Original Cassette Copy of Cassette I.D.

RELEASED TO

Name:	
Address:	
Postcode:	Telephone no:
Representative of: (Organisation/Company name if applicable)	
Signed:	
Released By (signed)	(printed)

RETURN OF RECORDING

Date: / /

Original Cassette Copy of Cassette I.D.

Returned By (signed)	(printed)
----------------------------	-----------------

Cassette Returned in Good Working Order (please tick)

Received By (signed)	(Operator Name)
----------------------------	-----------------------

CCTV SYSTEMS VISITORS / MAINTENANCE LOG

Sheet of

Date	Time	Name of Visitor	Sign In	Sign Out	Representative of:	Purpose of Visit / Work Carried Out
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						
...../...../.....						

CCTV CASSETTE STOCK CHECK & DISPOSAL LOG

Date of Check: / /

Carried Out By: (name) Signed:

CCTV Cassette ID (Please complete)	Location of Cassette (Please tick)	Condition of Cassette (Please tick)	Disposal Details (Please complete)
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:
.....	Locked Away <input type="checkbox"/> In Use <input type="checkbox"/> Missing Location Unknown <input type="checkbox"/>	Good <input type="checkbox"/> Fair <input type="checkbox"/> Poor <input type="checkbox"/>	Disposed of on: (date)/...../..... Method of disposal: Disposed of by:

THE PRINCIPLES OF DATA PROTECTION & THE CCTV CODE OF PRACTICE.

Introduction

In 1998, the scope of the Data Protection Act was broadened to enforce 8 principals of good practice regarding the personal data captured about individuals and how this is stored and processed. Personal data included facts and opinions about an individual.

It outlines that any organisation/individual or body who is collecting such information about people must then handle this data in an appropriate manner. Ie, that any data collected must be:

- ① fairly and lawfully processed,
- ② processed for limited purposes,
- ③ adequate, relevant and not excessive,
- ④ accurate,
- ⑤ not kept longer than necessary,
- ⑥ processed in accordance with the data subject's rights,
- ⑦ secure,
- ⑧ not transferred to countries without adequate protection.

Inevitably the capturing of personal data by means of a CCTV camera was more readily covered by the Act and closer monitoring of CCTV footage, it's usage and storage became paramount.

For a CCTV system owner, the Act essentially means that:

- they must register their CCTV system with the Information Commissioner,
- they must only take footage that is relevant to their property and it's security,
- they should not keep footage longer than it is necessary for a crime to come to light,
- they should warn individuals when they are in a monitored area,
- they should allow access to the footage to anyone who believes that they have been captured on one of the cameras,
- they should store captured footage securely so that access to it is strictly monitored.

By July 2000, just a few months after the Data Protection Act actually came into force, it became apparent that clearer guidelines were necessary to help CCTV system owners to run and manage their data storage more appropriately. For this reason, a CCTV Code of Practice was written by the Data Protection Commissioner as a guide to good practice for CCTV users. A summary follows:

A Summary

This is a summary of the code of practice issued by the Data Protection Commissioner. It is intended to provide guidance as to good practice for users of CCTV and other similar surveillance equipment.

It is not intended that the contents of this Code should apply to: -

- Targeted and intrusive surveillance activities, which are covered by the provisions of the forthcoming Regulation of Investigatory Powers Act.
- Use of surveillance techniques by employers to monitor their employees' compliance with their contracts of employment.
- It is intended that employers' use of personal data to monitor employee compliance with contracts of employment will be covered by the Data Protection Commissioner's forthcoming code of practice on use of employee personal data.
- Security equipment (including cameras) installed in homes by individuals for home security purposes. It is likely that the use of cameras by individuals to protect their own property is excluded from the provisions of the Act under the exemption at Section 36 of the Act.
- Use of cameras and similar equipment by the broadcast media for the purposes of journalism, or for artistic or literary purposes.

Following the 8 principals...

Before installing and using CCTV and similar surveillance equipment, users will need to establish the purpose for which they intend to use the equipment.

The First Data Protection Principle requires data controllers to have a legitimate basis for processing personal data, ie, images of individuals. This equipment may be used for a number of different purposes - for example, prevention, investigation and detection of crime, apprehension and prosecution of offenders, public and employee safety, monitoring security of premises etc.

If you are the Data Controller for your system, you must therefore:

- Establish who is the person(s) or organisation(s) legally responsible for the proposed scheme.
- Assess the purpose/reasons for using the CCTV equipment.
- Document these reasons.
- Ensure that notification is lodged with the Office of the Data Protection Commissioner covering the purposes for which this equipment is used.
- Establish and document the person(s) or organisation(s) who are responsible for ensuring the day-to-day compliance with the requirements of this Code of Practice (if different from above).

Siting the Cameras

This plays an important part of the Code as where the cameras are sited will determine which images are processed. Ideally, these images should only cover areas directly related to the purpose of the system. The Data Controller must ensure that the cameras are sited with this in mind.

- The equipment should be sited in such a way that it only monitors those spaces, which are intended to be covered by the scheme.
- If domestic areas such as gardens (or areas not intended to be covered by the scheme) border those spaces which are intended to be covered by the equipment, then the user should consult with the owners of such spaces if images from those spaces might be recorded.
- Operators must be aware that they are only able to use the equipment in order to achieve the purpose(s) for which it has been installed. If cameras are adjustable by the operators, this should be restricted so that operators cannot adjust or manipulate them to overlook spaces, which are not intended to be covered by the scheme.
- If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the scheme, then operators should be trained in recognising the privacy implications of such spaces being covered.
For example - it may be appropriate for the equipment to be used to protect the safety of individuals when using cash machines, but images of PIN numbers, balance enquiries etc should not be captured.

Signage

For a CCTV system to operate fairly under the Data Protection Act, the general public must be made aware of when data is being captured about them. CCTV Warning Signs are appropriate for this purpose as when an individual enters a camera zone, by having passed the warning sign they have given their consent to be filmed. Your Warning Signs must:

- Be clearly visible and legible to members of the public,
- Be an appropriate size for who is passing the sign. Eg, A4 size at eye level for someone passing the sign on foot or A3 for a driver entering a car park.
- Have a name and contact telephone number for the controller of the CCTV scheme.

Covert Installations

In certain instances, the use of signs may be inappropriate and jeopardise the purpose of the scheme. In this case the Data Controller must ensure that the CCTV cameras are operating under the following conditions:

- In areas where specific criminal activity has been identified.
- Where surveillance is required to obtain evidence of that criminal activity.
- Where the use of signs would prejudice success in obtaining evidence.
- For no longer a duration than necessary.

Quality of the Images

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose for which they are intended. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

The Data Controller must ensure that the system continually operates at an appropriate quality and accurately. Regular checks can be made to ensure that this is the case and these checks should be documented. An initial check should be undertaken to ensure that the equipment performs properly and the following points should be considered:

- If tapes are used, it should be ensured that they are good quality tapes. The cassettes on which the images are captured should be cleaned so that images are not recorded on top of images recorded previously.
- The cassettes on which the images have been recorded should not be used when it has become apparent that the quality of images has deteriorated.
- If the system records features such as the location of the camera and/or date and time reference, these should be accurate and their accuracy should be regularly checked and recorded.
- Cameras should be situated so that they will capture images relevant to the purpose for which the scheme has been established.
For example, if the purpose of the scheme is the prevention and detection of crime and/or apprehension and prosecution of offenders, the cameras should be sited so that images enabling identification of perpetrators are captured.
For example, if the scheme has been established with a view to monitoring traffic flow, the cameras should be situated so that they do not capture the details of the vehicles or drivers.
- When installing cameras, consideration must be given to the physical conditions in which the cameras are located. Eg, extra lighting or infra-red lighting may need to be installed to capture appropriate images.
- Users should assess whether it is necessary to carry out constant real time recording, or whether the activity or activities about which they are concerned occur at specific times.
For example - it may be that criminal activity only occurs at night, in which case constant recording of images might only be carried out for a limited period e.g. 10.00 pm to 7.00 am
- Cameras should be properly maintained and serviced to ensure that clear images are recorded.
- Cameras should be protected from vandalism in order to ensure that they remain in working order.
- A maintenance log should be kept.
- If a camera is damaged, there should be clear procedures for ensuring that the camera is fixed within a specific time period and monitoring the quality of the maintenance work.

Processing the images

Images, which are not required for the purpose for which the equipment is being used, should not be retained for longer than is necessary. While images are retained, it is essential that they are kept secure with limited access. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 1998 Act.

- Images should not be retained for longer than is necessary.
For example - publicans may need to keep recorded images for no longer than seven days because they will soon be aware of any incident such as a fight occurring on their premises.
For example - images recorded by equipment covering town centres and streets may not need to be retained for longer than 31 days unless they are required for evidential purposes in legal proceedings.
For example - images recorded from equipment protecting individuals' safety at cash machines might need to be retained for a period of three months in order to resolve customer disputes about cash withdrawals.
The retention period of three months is based on the interval at which individuals receive their account statements.
- Once this period has expired, the images should be removed or erased.
If the images are retained for evidential purposes, they should be retained in a secure place to which access is controlled.
- On removing the cassette on which the images have been recorded, the details should be documented.
This should include the date that the images were removed from the general system, the reason why they were removed from the system, any relevant crime incident number, the location where the images will be taken including who will view them, the signature of who has collected the cassette and the outcome of the viewing.
- Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed by anyone other than authorised employees of the user of the equipment.
- Access to the recorded images should be restricted to a manager or designated member of staff who will decide whether to allow requests for access by third parties in accordance with the user's documented disclosure policies.
- Viewing of the recorded images should take place in a restricted area, for example, in a manager's office.
Other employees should not be allowed to have access to that area when a viewing is taking place.
- All operators and employees with access to images should be aware of the procedure, which need to be followed when accessing the recorded images.

Access to and disclosure of images to third parties.

It is important that access to, and disclosure of, the images recorded by CCTV and similar surveillance equipment is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact should the images be required for evidential purposes. Users of CCTV will also need to ensure that the reason for which they may disclose copies of the images are compatible with the reason or purpose for which they originally obtained those images.

All employees should be aware of the restrictions set out in this code of practice in relation to access to, and disclosure of, recorded images.

- Access to recorded images should be restricted to those staff who need to have access in order to achieve the purpose of using the equipment.
- All access to the medium on which the images are recorded should be documented.
- Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances.
- All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented.
- Recorded images should not be made more widely available - for example they should not be routinely made available to the media or placed on the Internet.
- If it is intended that images will be made more widely available, that decision should be made by the manager or designated member of staff. The reason for that decision should be documented.
- If it is decided that images will be disclosed to the media (other than in the circumstances outlined above), the images of individuals will need to be disguised or blurred so that they are not readily identifiable.

Access by data subjects

There is a right in the 1998 Act to allow anyone believing that they have been captured on a CCTV camera to have access to that data. It is necessary for staff involved with the CCTV system at your premises to be aware of this right and to handle it appropriately.

Staff should be aware of the necessary procedure to be followed when a request is made and be able to provide the subject with a Subject Access Request Form. This may ask for the necessary information to find the images of the subject on the cassette, eg, the date & time when the individual believes that they have been captured, a photo if necessary. A charge of up to £10 may be made for such a search for images.

Individuals should also be provided with a leaflet, which describes the types of images, which are recorded and retained, the purposes for which those images are recorded and retained. This should be provided at the time that the standard subject access request form is provided to an individual.

The manager or designated member of staff should determine whether showing images to the individual would entail disclosing images of third parties. It may be necessary to consider here if a third party's privacy should be maintained. For example - it may be that members of the public whose images have been recorded when they were in town centres or streets have less expectation that their images are held under a duty of confidence than individuals whose images have been recorded in more private space such as the waiting room of a doctor's surgery.

If third party images are not to be disclosed, the manager or designated member of staff shall arrange for the third party images to be disguised or blurred.

If the manager or designated member of staff decide that the request will not be complied with, they must set out their reasons in the response to the individual.

If, within 21 days of that notification, the individual requires, in writing, the decision to be reconsidered, the manager or designated staff member shall reconsider the automated decision.

Monitoring compliance with this code of practice.

To ensure appropriate compliance with the Act, other matters to consider include:

- The contact point indicated on the CCTV Warning signs should be available to members of the public during office hours. Employees staffing that contact point should be aware of the policies and procedures governing the use of this equipment.
- A manager or designated member of staff should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with.