HANHAM FOLK CENTRE

CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM

POLICY OF OPERATION

April 2001

Approved by Management Committee

Drafted by K Lawrence **Signed:**

Approved on behalf of Management by **Signed:**

CONTENT

Authorised Personnel

The definitions in this document refer to a number of key personnel by title, this page identifies the holder of each of these posts.

Data Controller:	Trustees of the Hanham Folk Centre (The current Management Committee)
Officials:	Chairman, Vice-Chairman, Treasurer, Secretary, Administrator
Duty Officers:	Persons responsible for the building out of normal office hours.
Appointed Member:	Normally a member of Management committee who has been designated to this role and has the authority and responsibility defined in this document.

SCOPE

Under the Data Protection Act the Trustees of the Hanham Folk Centre are legally responsible for the CCTV system. Day-to-day compliance with the requirements of the Code of Practice lies with the Administrator, the duty Officers and the appointed member responsible for the CCTV system.

PURPOSE OF SCHEME

The CCTV system has been installed following a number of incidents where duty officers and staff have had unnecessary encounters with members of the public (primarily teenagers). A few of these incidents have resulted in the physical injury of members and staff. The CCTV scheme was installed to provide:

Objective 1: Public, Member and Employee Safety
Objective 2: Prevention and Detection of Crime
Objective 3: Apprehension and Prosecution of Offenders

Objective 1 was the primary reason for installing the system. The cameras were primarily located around the entrance area and know problem areas outside the building. This would provide the Duty Officer with a view outside the building and would record any incidents occurring in and around the entrance.

Additional benefits of the system are objectives 2 and 3. The presence of the CCTV system will provide a deterrent to crime out-of-hours and will allow a limited capability to detect and then prosecute offenders. Objective 2 and 3 were not the key driver for installing the system. In the future, the need to meet these may develop and the system may need extending.

OPERATION

The operation of the system is the responsibility of the Management Committee, who will normally delegate their authority and responsibility to a member. The appointed member is responsible for:

(1) Regularly checking system operation and performance.
(2) Annual replacement of tape pool.
(3) Accurate time and location information.
(4) Handling access requests for recorded images on video.
(5) System maintenance.
(6) Repair of damaged equipment in reasonable period of time.
(7) Training of duty officers and Administration staff.
(8) Maintenance the documentation for the system, which comprises:
    - Policy of Operation
        - Operators Instructions
        - Guidance Leaflet
        - Access Request Form
        - Complaints Procedure
    - Code of Practice
    - System Logbooks
    - Annual Effectiveness Report

RESPONSIBILITY OF DUTY OFFICERS AND ADMINISTRATOR

Principles

- All operators and employees with access to images should be aware of the procedures which need to be followed when accessing recorded images.

- All operators should be trained in their responsibilities under the Code of Practice. They should be aware of:-
  (a) Security policy eg procedures to have access to recorded images
  (b) Disclosure policy
  (c) Rights of individuals in relation to their recorded images

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

- All staff must be able to recognise a request from an individual to prevent processing likely to cause substantial and unwarranted damage to that individual.

Application

(A) Processing of Images (General)

RETENTION

- Images should not be retained for longer than is necessary. Images will be retained for a period not exceeding 31[1] days, unless required for evidential purposes or access request consideration.
- If the images are to be retained, they should be removed from the system and retained in a secure place such as a safe. This is the responsibility of the Administrator or appointed member.
- The official removing the images should ensure that they have documented the following:

Date removed	Time removed	Initials	Reason for removal	Related information: Crime number; Officers ID & name; Station where moved to; Signature of Officer. Access request info.

NOTE: If images are required by the police in the course of their enquiries, the tape containing the images should be handed to a police officer immediately. The officer will sign for the tape(s). The Police officers removing tapes from a scheme should be prepared to provide the scheme with a replacement tape.

- Where a tape is removed from the system, the replacement tape (whether provided by the police or stock) should be labelled as a temporary tape replacing tape Day **. i.e. Temp 01 replacing Day 10. This tape will be removed when the normal Day 10 tape has been returned; and has been record over.

[1] A pool of 31 videos is used such that video DAY1 is used on the first of the month. There will be instances when the DAY31 video will not be reused for a period of 61 days (Feb, Apr, June, Sept and Nov).

- Such tape replacements must be recorded in the CCTV logbook:

Date tape replaced	Time replaced	Initials of authorised person	Reason for replacement; Details: i.e. TEMP02 replaced DAY4; Location of DAY4 tape	Related information: Refer to another entry by date/time of incident of crime.
Date of return	Time of return	Initials of authorised person	Reason for return. Detail: DAY4 returned to replace TEMP02	Placed in storage unit below TEMP02. TEMP2 to be removed when DAY4 used.

ACCESS TO IMAGES

- Access to the recorded images should be restricted to an official or appointed member who will decide whether to allow requests for access by third parties in accordance with the documented disclosure policy described in the Policy of Operation.
- Viewing of the recorded images will take place in the office with no unnecessary observers. Other employees should not be allowed to have access to that area when a tape is being viewed.
- Removal of the images for viewing should be documented as follows:

Date removed	Time removed	Initials of remover	Reason for removal and viewing; Approving persons name; Requesters Name	Outcome of viewing; Time tape was returned to storage; Type of ID provided.

- All access to images must be documented.

(B) Disclosure of Images to Third Parties

- Access to images by third parties should only be allowed in limited and prescribed circumstances. If the purpose of the system is the prevention and detection of crime, then disclosure to third parties should be limited to the following:-

  (a) law enforcement agencies where the images recorded would assist in a specific criminal enquiry

  (b) prosecution agencies

  (c) legal representatives

  (d) the media, where it is assessed by the police that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment, the wishes of the victim of an incident should be taken into account

  (e) the people whose images have been recorded and retained (unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings.
- All requests for access or for disclosure should be recorded. If access or disclosure is denied, the reason should be documented in the CCTV Logbook. The release of any images must be approved. For the provision of images to a law enforcement agency this can be approved by an officer, the administrator or a duty officer. All other requests must be addressed by the Data Controller.
- Recorded images should not be made more widely available.
- When access to or disclosure of the images is allowed or denied, then the following should be documented, respectively:

Date of access and disclosure	Time of access and disclosure	Initials of manger	Reason for removal and viewing; Extend of access; Approving person's name.	Outcome of viewing; Time tape was returned to storage; Type of ID provided.
Date of denial	Time of entry	Initials of logger	Reason for refusal.	Outcome from requester.

NOTE: If images are required by the police in the course of their enquiries, the tape containing the images should be handed to a police officer immediately. The officer will sign for tape(s). The Police officers removing tapes from a scheme should be prepared to provide the scheme with a replacement tape.

- Where a tape is removed from the system, the replacement tape (whether provided by the police or stock) should be labelled as a temporary tape replacing tape Day **. i.e. Temp 01 replacing Day 10. This tape will be removed when the normal Day 10 tape has been returned; and has been record over.
- See table on page 6.

(C) Access by Data Subjects

- Data subjects should be provided with a standard subject access request form which :-
  (a) indicates the information required in order to locate the images requested.
  (b) indicates the information required in order to identity the person making the request.
  (c) indicates the fee that will be charged for carrying out the search for the images requested.
  (d) asks whether the individual would be satisfied with merely viewing the images recorded.
- 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, and information about the disclosure policy in relation to those images.
- This should be provided at the time that the standard subject access request form is provided to an individual.
- All subject access requests should be dealt with by the data controller(s).
- The official or appointed member should determine whether disclosure to the individual would entail disclosing images of third parties and inform the data controller(s).
- The data controller(s) should determine whether or not to disclose the images of third parties.
- Once approved for release, the official or appointed member should locate the images requested.
- If the data controller(s) decide that a subject access request from an individual is not to be complied with, the following should be documented:

Date of entry	Time of entry	Initials of logger	Name of requester; Date of request; Detail of request.	Reason for refusal; Name & sign of person authorised to refuse access.

- All staff should be aware of individuals' rights under this section of the Code of Practice.

Operation Procedures

The day-to-day operation of the system by the authorised officers is detailed below, and is summarised in the CCTV logbook.

(1) Evening Tape Changes

The CCTV video records for 24 hours on a single tape. The tapes must be changes once a day at approximately 7pm.

Procedure
TO BE COMPLETED BEFORE OPENING THE BUILDING TO MEMBERS OR THE PUBLIC

- Lower Flap of Video Recorder and press <**REC LOCK**> located at the right.
- Press the <**STOP**> button to stop recording.
- Press <**REWIND**> to rewind the tape.
- When the tape is fully rewound press <**EJECT**>.
- Replace the tape in the cardboard dust cover and insert it into the top of the storage unit.
- Unlock the lower slot of the storage unit and remove the next video.
- Check the label on the tape corresponds to the date (i.e. DAY 10 for 10th March).
- For the first day of the month you may have to place one or more videos in the top slot and remove videos from the bottom slot to reach DAY 1.
- Once you have the correct video, lock the lower slot.
- Insert the video into the recorder.
- Press <**REC**> to start recording and check the RED record symbol is lit and the counter is counting.
- Press <**REC LOCK**> to lock recording and close the lower flap.
- Enter the following information in the CCTV logbook.:

Date changed	Time changed	Initials of changer	Reason: Changed tape to Day 12	Detail: Signature

Temporary Video Tapes

When extracting videos from the storage unit, you may encounter a temporary tape. These are used to replace a tape from the normal pool of DAY** videos when it has been:

(1) Submitted to police as evidence;
(2) Retained in secure storage following a request from a Data Subject;
(3) Retained in secure storage following a complaint.

Procedure

- If a temporary video is taken from the bottom slot for an evening change, it will be labelled:

  Temp ** replacing DAY ** (i.e. TEMP01 replacing DAY12)

- If DAY** (12 in the above example) is the expected tape, and the next video showing in the storage unit is DAY**+1 (i.e. 13) then proceed as normal using TEMP** (01) in place of the DAY** (12) video.

Exception

- If a DAY** video is removed from lower slot of the storage unit, and is followed by a temporary video (Labelled TEMP** replacing DAY **) where the DAY of the temporary video matches that of the normal video. i.e. A DAY14 video is extracted and is followed by a "TEMP02 replacing DAY14" video.
- In this case, use the DAY** video, and leave a note for the Administrator regarding the temporary video (This will be removed from the system, as the DAY** video has now been returned and used).
- Record all temporary videos in the CCTV logbook:

Date changed	Time changed	Initials of changer	Reason: Change of tape to Day 12 (Used TEMP02 replacing DAY12)	Detail: Signature
Date changed	Time changed	Initials of changer	Reason: Changed to tape DAY15 (TEMP04 replacing DAY15 in lower slot); Left note for administrator	Detail: Signature
Date	Time	Initials of Official	Reason: Removed TEMP04 from storage following return and usage of DAY15.	Detail: Signature

(2) Viewing the Live Cameras

Whilst the multiplexer offers a wide range of options, it is essential that this unit is not used improperly as this could stop the cameras being recorded correctly. Only use the Function Keys (F1 to F8) on the left-hand side of the control unit. Do not use the main keyboard.

F1	Quad Split I (DEFAULT)	F2	Quad Split II
F3	Full Screen Sequence (1 sec)	F4	Full Screen Sequence (5 sec)
F5	Picture-in-Picture (4)	F6	Full Screen Seq (5 sec) *{Covert}*
F7	Multi-screen (8/2) {Road}	F8	Multi-screen (8/2) {Building}

Pressing the HOLD button while in FULL SCREEN mode freezes the image on the screen. Press HOLD again to release.
NOTE: For Function Keys F3, F4 and F6 you may need to press the key twice to enable Sequencing of the images.

Do not use any other features of the system

(3) Recording an Incident

If an incident occurs during a period when the centre is occupied it is important this is recorded in the CCTV logbook to allow it to be easily located at a later date.

- Record the following information in the logbook:

Date of incident	Time of incident	Initials of logger	Detail and location of incident. Cameras involved.	Video counter number; Duration of incident

(4) Handling Complaints and Queries

Other than the live quad-display on the office monitor and the foyer image displayed on the awareness spot monitor, normal members and the public do not have an instant right to view camera images or recorded information.

COMPLAINTS
Complaints regarding the use of the system or complaints regarding any non-compliance with the CCTV code of practice should be handled by reference to the Complaints section of the Policy of Operation document. Any complaint should be recorded in the logbook.

REQUEST FOR DATA
All requests for access or for the disclosure of data should be recorded in the logbook.

(1) Request for access to data by a recorded subject. Persons making a request to view recorded images must be given an Information leaflet and Access Request Form (Annex A). Requests will be passed the Management committee for a decision and will be addressed within 8 weeks. In the interim, an official or the appointed member will remove any related videos to a secure location.

(2) Requests to prevent processing or recording must be presented in writing and will be addressed within 21 days by the Management committee.

(3) Requests by Third parties. (i.e. Police). These must be approved prior to the provision of data, the information required is defined elsewhere in this document and should be recorded in the CCTV logbook. The release of images to the authorities is to be approved by an official or appointed member.

(4) Disclosure of Third party images. The official or the appointed manager will determine if an image can be released depended on whether the image(s) of any third party persons is considered unsuitable for release.

(5) Code of Practice. The public or members can request a copy of the Code of Practice for CCTV usage. This can be viewed in the office or the person can obtain a copy from the Data Protection Act web site.

Type of Request	Action	Authority to Access Request
From Data Subject	Provide leaflet and Access Request Form; Log Request in CCTV Logbook; Remove video to secure location.	Management Committee
From Third Parties (i.e. Police)	Record request in CCTV Logbook; Remove video to secure location.	Administrator, Official, Appointed member.
To prevent processing	Record request in CCTV logbook; Advise requester to put request in writing.	Management Committee
Request for code of Practice	Code of Practice can be viewed in the Office (ONLY). Public can obtain copies from Data Protection Agency.	None
Complaint	See below.	Management Committee

COMPLAINTS PROCEDURE

Complaints fall into two categories:
(1) Complaints about the use of the system
(2) Complaints about any non-conformance with the CCTV Code of Practice

Both types of complaint are to be handled in the same manner.

Procedure

- Complaints must be provided in writing.
- Record details of the complaint in the CCTV logbook as follows:

Date of complaint	Time of complaint	Initials of logger	Detail and location of incident. Details of requester.	Any comments. Record if written request received.

- The administrator will remove the tape from the storage unit to a secure place and replace it with a Temp tape (Labelled Temp02 for Day 14). Once the incident has been resolved the tape Day 14 will replaced after it has been recorded on (i.e. on day 15).
- Full details of tape replacement should be recorded in the CCTV logbook. (see table on page 6).
- Pass the written complaint to the administrator; or advice of pending complaint.
- The administrator will notify the appointed member.
- The administrator will pass the complaint to the Management committee for action.
- Details of the response should be recorded in the CCTV logbook.
- The complainant must be informed (in writing) of the outcome within 8 weeks of receipt of the complaint.
- The complainant should be informed that if they are not satisfied with the response they should seek further clarification and/or they can contact the Data Protection Agency to seek further advice.

ANNEX A

COMPLIANCE WITH THE CODE OF PRACTICE

- ✓ The contact point indicated on the sign should be available to members of the public during office hours (Administrator).

- ✓ They should be provided, on request with one or more of the following:-
  - ➢ The leaflet which individuals receive when they make a subject access request as general information.
  - ➢ A copy of this code of practice.
  - ➢ A subject access request form if required or requested.
  - ➢ The complaints procedure to be followed if they have concerns about the use of the system or if they have concerns about non-compliance with the provisions of this Code of Practice.

- ✓ A complaint procedure should be clearly documented.

- ✓ A record of the number of complaints or enquiries should be maintained.

- ✓ A report on those numbers should be collected by the administrator or appointed member in order to assess public reaction to and opinion of the use of the system.

- ✓ An official or appointed member should undertake regular reviews of the documented procedures to ensure that the provisions of this Code are being complied with.

- ✓ A report on those reviews should be provided to the data controller(s) in order that compliance with legal obligations and provisions with this Code of Practice can be monitored.

- ✓ An annual report should be produced which evaluates the effectiveness of the system. This report should be assessed against the stated purpose of the scheme. If the scheme is not achieving its purpose, it should be discontinued or modified.

- ✓ Those reports should be made publicly available.

Annex B: Data Protection Principles

FIRST DATA PROTECTION PRINCIPLE

This requires that

"Personal data shall be processed fairly and lawfully, and, in particular, shall not be processed unless-

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met".

THE SECOND DATA PROTECTION PRINCIPLE

This requires that

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

THE THIRD DATA PROTECTION PRINCIPLE

This requires that

"Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

THE FOURTH DATA PROTECTION PRINCIPLE

This principle requires that

"The personal information that is recorded and stored must be accurate."

THE FIFTH DATA PROTECTION PRINCIPLE

This principle requires that

"The information shall not be held for longer than is necessary for the purpose for which it is to be used."

THE SIXTH DATA PROTECTION PRINCIPLE

The Act provides individuals with a number of rights in relation to the processing of their personal data: -

- the right to be provided, in appropriate cases, with a copy of the information constituting the personal data held about them
- the right to prevent processing which is likely to cause damage or distress
- rights in relation to automated decision-taking
- the right to seek compensation for damage and distress suffered as a result of any contravention of any of the requirements of the Act

THE SEVENTH DATA PROTECTION PRINCIPLE

This requires that

"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".

THE EIGHTH DATA PROTECTION PRINCIPLE

This Principle places limitations on the ability to transfer personal data to countries and territories outside of the EEA.

Annex C

Hanham Folk Centre - CCTV System

Information Leaflet and Access Request Form

Background

Under the Data Protection Act the Trustees of the Hanham Folk Centre are legally responsible for the CCTV system. Day-to-day compliance with the requirements of the Code of Practice lies with the Administrator, the Duty Officers and the appointed member responsible for the CCTV system.

The CCTV system has been installed following a number of incidents where duty officers and staff have had unnecessary encounters with members of the public (primarily teenagers). A few of these incidents have resulted in the physical injury of members and staff. The CCTV scheme was installed to provide:

Objective 1: Public, Member and Employee Safety
Objective 2: Prevention and Detection of Crime
Objective 3: Apprehension and Prosecution of Offenders

Images Recorded and Retained

Images from all cameras on the system are recorded 24 hours per day, 365 days per year. Images are normally retained on video tape for a period not exceeding 31 days. Video tapes are held within a secure area and access is controlled in line with the code of practice. Images retained are of sufficient clarity and definition to identify individuals.

Disclosure Policy

Both live and recorded images (other than those on the spot monitor) will not be disclosed to anyone who does not have authority to control the images. Duty officers do not have the authority to display/release any images. All requests for data must be handled using the procedures laid down in the CCTV Policy of Operation.

Details of the system beyond that specified herein are, in the interests of the Folk Centre's security, considered confidential.

Access Requests

Under the Data Protection Act the data controller is responsible for the measures to be taken against the unauthorised or unlawful processing and release of personal data (which includes facial CCTV images). As such requests for access to recorded images must be handled formally, fairly and effectively. All requests for data must be on the attached Access Request Form, they must be accompanied by the payment of the search fee (£10) and proof of ID (Validated membership card, driving licence, photo credit card or passport).

If approved, a time and date to view the images will be agreed and the requester will be asked to view the images with a representative of the data controller. If unsatisfied, the requester can follow the complaints procedure. A request for further data will be not approved until a suitable period has passed and a further fee has been paid.

Access Request Form

Note: Images are normally retained for a period not exceeding 31 days.

Details of Requester:

Name: _____ Date: _____

The image(s) requested is/are of ☐ myself ☐ a relation ☐ a 3rd party

Details of image(s) requested:

Date(s) required: _____ Time: _____

_____ _____

Camera/Location: _____

_____

_____

_____

Reason for request(s): _____

_____

_____

_____

Payment of search and display fee (£10):

Enclosed: ☐ Yes ☐ No

Office Use Only:

Video identified and moved to Secure Storage: ☐ Yes ☐ No

Video Number(s) Moved: _____ _____ _____

Temporary Replacements: _____ _____ _____

Carried out by: _____ (Signed)

Request Approved: ☐ Yes ☐ No Meeting Date: _____

Agreed date and time for display of image(s): _____

Proof of Requesters ID: _____

Completed: Signed: _____(requester) Date: _____

Signed: _____(For Centre)

Proof of ID should accompany form along with payment of fee.

ANNEX D

SAMPLE CCTV LOGBOOK ENTRIES

Date	Time	Initials	Action; Reason	Comments; Information; Outcome; Signatures
24/01/02	19:03	SEW	Changed tape to day 24	Signature
25/01/02	19:05	SEW	Changed tape to day 25	Signature
26/01/02	18:58	EJS	Changed tape to day 26	Signature
26/01/02	20:10	EJS	Minor incident outside	Counter: 2345
26/01/02	22:18	EJS	Major incident outside; Camera 1 & 2	Counter: 2858 Police Incident: 34523 Officer: P Plod requested Tape
27/1/02	10:11	SN	Removed and provided video (DAY 26) to Police.	Officer: P Plod ID: 3456 Taken to Staple Hill <Signed>
27/01/02	10:20	SN	Replaced DAY26 with (TEMP01 replacing DAY26) in storage unit	Signature
27/01/02	19:03	WEG	Changed tape to day 27	Signature
28/01/02	18:52	RDJ	Changed tape to day 28	Signature
28/01/02	22:50	RDJ	Minor incident in Bar	Counter: 4512 Bar Camera
29/01/02	10:00	SN	Complaint about usage received from <name>	Passed to management to address.
29/01/02	10:10	SN	Tape DAY28 placed in safe. Replaced DAY26 with (TEMP02 replacing DAY26)	Signature
29/01/02	19:03	RS	Changed tape to day 29	Signature
30/01/02	18:49	EJS	Changed tape to day 30	Signature
31/01/02	10:00	KML	Removed tape day 30 Inserted tape TEST	Check and tested system operation
31/01/02	10:21	KML	Replaced tape day 30 in recorder	Signature
01/02/02	07:03	EJS	Changed tape day 01	Signature
02/02/02	07:09	RS	Changed tape day 02	Signature
03/02/02	06:57	RS	Changed tape day 03	Signature
03/02/02	08:04	RS	Request for Image from <name>	Provided copy of Info leaflet & Access request form.
04/02/02	09:36	SN	Received access Request form. Removed tape day 12 from storage unit. Replaced with (TEMP03 replacing DAY12)	Request passed to Management Committee
04/02/02	19:02	SN	Changed tape to day 04	Signature
05/02/02	12:20	SN	Police returned tape Day 26. Placed in storage unit (TEMP1 also in unit).	TEMP01 will be removed on 27 Feb 02, after DAY26 has been used.
05/02/02	19:02	EJS	Changed tape to day 05	Signature
06/02/02	18:56	EJS	Changed tape to day 06	Signature