HANHAM COMMUNITY CENTRE

A Charitable Incorporated Organisation - Charity No. 1152575

CLOSED CIRCUIT TELEVISION (CCTV) SYSTEM

POLICY OF OPERATION

October 2017

V2.3

Approved by Board of Trustees – October 17
Revalidated: Oct 2017

Approved on behalf of Board of Trustees **Signed:**

AMMENDMENTS

Version	Date	Author	Comments
0.1A	Feb 01	K M Lawrence	Initial Draft
1.0	Apr 01	K M Lawrence	Issued Document
1.5	Aug 02	K M Lawrence	Minor Revisions
0.2A	Jul 07	K M Lawrence	V2.0 Draft
2.0	Aug 07	K M Lawrence	Minor corrections and Issued
2.1	Mar 09	K M Lawrence	Centre Name Change
2.1	Jan 13	K M Lawrence	Revalidated
2.2	Aug 13	K M Lawrence	Revised Charity Number
2.3	Oct 17	K M Lawrence	Revalidated and minor updates

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 Community Centre (The current Board of Trustees)
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 Board of Trustees who has been designated to this role and has the authority and responsibility defined in this document.

1. SCOPE

Under the Data Protection Act the Trustees of the Hanham Community 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.

2. 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[1]
Objective 3: Apprehension and Prosecution of Offenders
Objective 4: Visibility around and within the building from the main office in support of Objectives 1-3.

Objective 1 was the primary reason for installing the system. The cameras were primarily located around the entrance area and known 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 cameras have been installed within the building to provide staff with a clear view of the key public areas, and these are likely to be extended in the future – covert cameras may be used (Objective 4). CCTV images may also be used as evidence in staff disciplinary matters. The system does not (formally) cover the Car Park.

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. Since the installation of this system, it has provided CCTV information in support of many incidents and has been used to prosecute Offenders.

3. OPERATIONAL RESPONSIBILITY

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

(1) Regularly checking system operation and performance
(2) Accurate time and location information
(3) Handling access requests for recorded images on video
(4) System maintenance and control over access to the system
(5) Repair of damaged equipment in reasonable period of time
(6) Training of duty officers and Administration staff
(7) Maintenance the documentation for the system, which comprises:

- Policy of Operation
  - Guidance Leaflet Annex C
  - Access Request Form Annex C
  - Complaints Procedure
- Compliance to Code of Practice Annex A
- System Logbooks
- Systems Effectiveness Report Annex E

[1] This is also addressed by the 2003 Licensing Act and HFC includes the CCTV system as a preventative measure applied to aid compliance with the four licensing objectives.

4. STAFF AWARENESS

- 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 (though not necessarily recording) likely to cause substantial and unwarranted damage to that individual.

5. PROCESSING, RETENTION AND ACCESS

(A) Processing of Images

(A1) RETENTION OF IMAGES

- Images should not be retained for longer than is necessary. Images will be retained for a period of approximately 31[2] days, unless required for evidential purposes or access request consideration.
- If the images are to be retained, they should be removed from the system[3] 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 images will be extracted by the appointed members and provided to the police. The officer will sign for the media/images in the logbook.

(A2) 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 at a location with no unnecessary observers. Other employees should not normally be allowed to have access to that area when a tape is being viewed.

[2] This is dependent on the activity in a period, and may fluctuate from 20 days to 45 days; but is nominally around 30 days. The data is written to a hard disk unit and is continually overwritten.
[3] Images may be transferred to computer, CD or other media; or still images may be printed.

- The CCTV system may be accessed remotely by appointed officials to allow monitoring of the live system; as well as the display, searching, processing and extraction of video or still images.
- 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; Media image transferred to & duration, number of images etc. Type of ID provided.

(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 appointed member.
- Recorded images should not be made more widely available – general 'public views' may be approved for release for demonstration purposes as 'examples' of the systems capability – usually as part of maintenance and testing.
- 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; 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 images will be extracted by the appointed members and provided to the police. The officer will sign for the media/images in the logbook.

(C) Access by Data Subjects

- Data subjects should be provided with an Access Request Form (Annex C) which :-
  (a) indicates the information required in order to locate the images requested.
  (b) indicates the information required in order to identify 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.
  (e) indicates a justifiable reason for the extraction and viewing of 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, 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 appointed member.
- 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 appointed member should determine whether or not to disclose the images of third parties – this may be referred to the Board of Trustees for a decision.
- Once approved for release, the official or appointed member should locate the images requested.
- If it is decided 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.

6. OPERATION PROCEDURES

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

(A) Normal Operations

The CCTV system has a maximum of 16 cameras, and records the images (in colour where colour cameras have been deployed) to a hard disk unit within the system. This (nominally) will hold 15 days of recording and will overwrite the oldest images as it records the current 'live' images. The system (nominally) records at 1 fps, but where motion is detected can increase the frame rate and resolution. The schedule of operations is defined by the Appointed Member and is backed-up onto a computer.

There is no operator involvement in the day-to-day recording of images.

(B) Viewing the Live Cameras

Whilst the system 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. In normal operation the monitor displays current images from all (or most) cameras – this may alter at different times of day.

Individual cameras can be displayed by double clicking the select camera's image, whilst multiscreen images can also be selected and sequenced. Some cameras may be defined as covert and their images will not be shown (though will be recorded).

The main functions (including remote access across the LAN and WAN) are password protected. Remote access also requires knowledge of the CCTV's external DNS address and the devices port number.

Do not use any other features of the system

(C) 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.	Exact time display on CCTV monitor. Duration of incident Dd/mm/yy-hh:mm:ss

(D) 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 this Policy of Operation document. Any complaint should be recorded in the logbook.

(E) Queries and Requests for Data

Other than the live multi-display and motion display on the office monitor, normal members and the public do not have an instant right to view camera images or recorded information. All queries, 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 to the appointed member for a decision and will be addressed within 8 weeks. In the interim, an official or the appointed member will (where possible) copy any related images to a secure location.

(2) Requests to prevent processing or recording (for a well defined reason) must be presented in writing and will be addressed within 21 days by the Board of Trustees.

(3) Requests by Third parties. (i.e. Police). These will be approved by an official or the appointed member and will be provided as soon as possible to the requesting authority – noting not all staff have access to the system. The information required is defined elsewhere in this document and should be recorded in the CCTV logbook.

(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 obtain a copy of the Code of Practice for CCTV usage from the Data Protection Act web site. A copy of our compliance with this Code of Practice is shown at Annex A.

Type of Request	Action	Authority to Access Request
From Data Subject	Provide leaflet and Access Request Form; Log Request in CCTV Logbook; Remove images to secure location asap.	Appointed Member (Board of Trustees)
From Third Parties (i.e. Police)	Record request in CCTV Logbook; Remove images to secure location asap.	Administrator, Official, Appointed member.
To prevent processing	Record request in CCTV logbook; Advise requester to put request in writing.	Board of Trustees
Request for code of Practice	Compliance with the code of Practice can be viewed at Annex A. The Code of Practice is available from the Data Protection Agency website.	None
Complaint	See below.	Board of Trustees

7. 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/appointed member will endeavour to copy the images to alternative media. Once the incident has been resolved the images will be retained for a further 12 weeks and then removed.
- 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 Board of Trustees 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.

- ✓ A 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 Community Centre - CCTV System

INFORMATION LEAFLET & ACCESS REQUEST FORM

Background

Under the Data Protection Act the Trustees of the Hanham Community 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 system is registered under the Data Protection Act.

The CCTV system was installed following incidents (on and off the premises) 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 4:	Visibility around and within the building from the main office in support of Objectives 1-3.

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 hard drives (computer disks) for a period (nominally) of 15 days. Images retained are of sufficient clarity and definition to identify individuals. Images are record in High Defintion colour; cameras are located around the perimeter and within the building. Covert cameras may be used.

Disclosure Policy

Both live and recorded images (other than those on the 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 recorded images. All requests for data must be handled using the procedures laid down in the CCTV Policy of Operation. Remote access to the system can be provided to approved persons whereby they can view live & recorded images. Details of the system beyond that specified herein are, in the interests of the Centre's security, confidential. 'Public views' may be provided as 'examples' of the systems capability and will be released by the authorised member.

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. 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 not be approved until a suitable period (4 weeks) has passed and a further fee has been paid.

HANHAM COMMUNITY CENTRE – CCTV SYSTEM

HFC is a Registered CIO Charity No. 1152575

ACCESS REQUEST FORM

Note: Images are retained for a period (nominally) of 15 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:

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

Start Date-Time: _____
dd/mm/yyyy-hh:mm:ss

Finish Date-Time: _____
dd/mm/yyyy-hh:mm:ss

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
26/01/12	20:10	LP	Minor incident outside	26/01/02-20:02:20
26/01/12	22:18	DC	Major incident outside; Camera 1 & 2	26/01/02-21:45:34 Police Incident: 34523 Officer: P Plod requested images
27/1/12	10:11	KML	Removed and provided CD to Police. (15 mins video) + 5 still images.	Officer: P Plod ID: 3456 Taken to Staple Hill <Signed>
28/11/12	22:50	TC	Minor incident in Bar (5 mins)	28/01/02-22:45:14 Bar Camera
29/11/12	10:00	JC	Complaint about usage received from <name>	Passed to BOT to address.
31/01/13	10:00	KML	System test and checks	Check and tested system operation
03/02/13	08:04	SM	Request for Image from <name>	Provided copy of Info leaflet & Access request form.
04/04/13	09:36	JC	Received access Request form. Transferred 10 mins of video to computer.	Request passed to BOT. 03/02/02-07:10:14 – 03/02/02-07:20:25
15/02/14	09:15	JC	Incident. KML remotely transferred images to CD.	15/02/02-03:00:00 – 15/02/02-03:15:00
15/02/16	10:00	JC	Still images emailed to ASP[4]	<email address>
25/03/17	21:00	TC	Minor incident in foyer	25/02/02-20:07:04

[4] ASP – Avon & Somerset Police

ANNEX E

SYSTEM EFFECTIVENESS REPORT

Objective 1:	Public, Member and Employee Safety
Objective 2:	Prevention and Detection of Crime
Objective 3:	Apprehension and Prosecution of Offenders
Objective 4:	Visibility around and within the building from the main office in support of Objectives 1-3.

HCC has operated a CCTV system since March 2017, with the current High Definition Digital CCTV system being installed between 2015 and 2017, and during this time is had had a significant impact on the safety and security of the premises, staff and users. Whilst some users may consider it an intrusion, the coverage of open public areas has provided an effective deterrent of inappropriate behaviour by a range of people.

Since the installation, the system has provided a large number of images to the police in furtherance of the detection of criminal activities, both off and on the premises and it has been used to provide evidence on 'frays of the peace' within the building.

In terms of the Objectives, it is the opinion of the Trustees that the system provided an effective means of maintaining public, member and employee safety (Obj 1) and that this has been greatly improved by the addition of camera both within and around the building, as well as the adoption of colour cameras (Obj 4). The considerable number of images provided to the police provided evidence that Obj 2 and 3 have been effectively addressed. Day time coverage has also permitted the office to remove some personnel from within the building (Obj 2 & 4).

In summary it is the opinion of the Trustees that the system is proving effective at meeting the Objectives defined and will continue to be operated and maintained.

Future

The system is capable of supporting 16 cameras, it is the aspiration of the Trustees to extend the coverage of the external cameras to provide better coverage of the north and east sides of the building. It is also intended to provide additional internal cameras to cover all the main corridors and entry/exit points. This will be subject to funding and project prioritisation.

It would (potentially) be possible to extend the system (or part thereof) to be included in any future Hanham High Street CCTV surveillance system as well as extend it to cover the Sports Pavilion.