Florence Park Community Association
CCTV POLICY

Date Ratified:	August 2025
Next Review Date:	June 2027
Organisation Name:	Florence Park Community Association, Charity No. 1159506
Designated Data Protection Officer:	Adam W (contact florenceparkcommunitycentre@gmail.org)

1 Policy Statement

Florence Park Community Association (FPCA) uses Close Circuit Television ("CCTV") on the premises.

The purpose of this policy is to set out the position of FPCA as to the management, operation and use of the CCTV across Florence Park Community Centre (FPCC).

This policy applies to all members of our workforce, visitors to FPCC and its surrounding area and all other persons whose images may be captured by the CCTV system.

This policy takes account of all applicable legislation and guidance, including:

- General Data Protection Regulation ("GDPR")
- Data Protection Act 2018 (together the Data Protection Legislation)
- CCTV Code of Practice produced by the Information Commissioner
- Human Rights Act 1998

This policy sets out the position of FPCA in relation to its use of CCTV.

2 Purpose of CCTV

2.1 FPCA will use CCTV for the following purposes:

- To provide a safe and secure environment for staff and visitors
- To prevent the loss of or damage to the building and/or assets
- To assist in the prevention of crime and assist law enforcement agencies in apprehending offenders
-

3 Description of System

Some of the areas will have a number of cameras in and outside of the building. Some cameras have sound recording capabilities and there is a range of movable and fixed cameras.

Key attributes of the system are detailed in the table below:

CCTV System Manufacturer:	UNV

Maximum Channel Capacity:	16 maximum – 14 currently in use
Disk Space and Recording Retention Period:	4TB Raw – 3726GB Formatted 14-30 days
Number of Cameras on-site:	14
Resolution of Cameras:	• High quality image with 4MP, 1/3" CMOS sensor**4MP (2688 × 1520)@25/20 fps**; 4MP (2560 × 1440)@25/20 fps; 3MP (2304 × 1296)@30/25 fps; 2MP (1920 × 1080)@30/25 fps (default is in bold) • Ultra 265, H.265, H.264, MJPEG • 120 dB true WDR technology enables clear image in strong light scene • Support 9:16 Corridor Mode • Built-in Mic and Speaker • Smart IR, up to 30 m (98 ft) IR distance • White Light, up to 30 m (98 ft) warm light distance
Location of Recording Device:	In 'The Office'
Installation Company:	Enter-at
Installation Date:	30/7/25

4 Siting of Cameras

All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff and visitors.

Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. FPCA will make all reasonable efforts to ensure that areas outside of the premises and grounds are not recorded.

Signs will be erected to inform individuals that they are in an area within which CCTV is in operation.

Cameras will not be sited in any areas where members of staff have an expectation of privacy, such as changing rooms or toilets.

Cameras may be located in communal areas and, where this is the case, visitors and members of staff will be made aware. Access to the footage is restricted and will only be used to fulfil the purposes in 2.1.

5 Privacy Impact Assessment

Prior to the installation or repositioning of any CCTV camera, or system, a privacy impact assessment will be conducted by FPCA to ensure that the proposed installation is compliant with legislation and ICO guidance.

FPCA will adopt a privacy by design approach when installing new cameras and systems, considering the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.

6 Management and Access

The CCTV system within the FPCA will be managed by the Centre Manager.

Any allegations against FPCA/FPSC staff will be referred immediately to the Centre Manager and only (s)he will determine who needs to view the footage and the course of action necessary. Any issue will be referred to the Community Association Chair as appropriate.

On a day-to-day basis the CCTV system will be operated by individuals who have been specifically trained in the operation of the system and are both competent and considered to have the appropriate technical ability.

The viewing of live CCTV images will be restricted to the Centre Manager, FPCA management team, FPSC management team and Enter-At. In doing so they will ensure that the purposes in 2.1 are satisfied.

Recorded images which are stored by the CCTV system will be restricted as in 6.4. Relevant images may be shared with the leadership teams allowing them to review incidents where disciplinary matters or complaints need to be addressed.

No other individual will have the right to view or access any CCTV images unless in accordance with the terms of this policy as to disclosure of images.

The CCTV system will be checked regularly to ensure that it is operating effectively.

7 Storage and Retention of Images

Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.

Recorded images are stored for a maximum of 30 days unless there is a specific purpose for which they are retained for a longer period. If images need to be retained, they will be copied onto an external device which will be wiped clean once any image review has been completed.

FPCA will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:

- CCTV recording systems being located in restricted access areas;
- The CCTV system being encrypted/password protected;
- Restriction of the ability to make copies to specified members of staff

A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by FPCA.

8 Disclosure of Images to Data Subjects

Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images.

Any individual who requests access to images of themselves will be considered to have made a subject access request (SAR) pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Trust's Subject Access Request Policy.

When such a request is made the appropriate individual with access to the CCTV footage (ref 6.4) will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.

If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The individual accessing the footage must take appropriate measures to ensure that the footage is restricted in this way.

If the footage contains images of other individuals, then FPCA must consider whether:

The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

A record must be kept, and held securely, of all disclosures which sets out:

- When the request was made;
- The process followed by to the individual with access to the CCTV footage in determining whether the images contained third parties;
- The considerations as to whether to allow access to those images;
- When the individuals that were permitted viewed the images
- Whether a copy of the images was provided, and if so to whom, when and in what format.

Note that, when a subject access request is made then, unless an exemption applies (such as in relation to third party data that it would be unreasonable to disclose) then the requester is entitled to a copy in a permanent form. There is reference here only to "access" as opposed to a "permanent copy" as FPCA may consider it preferable in certain circumstances to seek to allow access to images by viewing in the first instance without providing copies of images. If an individual agrees to viewing the images only then a permanent copy does not need to be provided. However, if a permanent copy is requested then this should be provided unless to do so is not possible or would involve disproportionate effort.

9 Disclosure of Images to Third Parties

FPCA will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.

CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.

If a request is received from a law enforcement agency for disclosure of CCTV images, then the individual with access to the CCTV footage must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.

The information above must be recorded in relation to any disclosure.

If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

10 Review of Policy and CCTV System

This policy will be reviewed every two years or earlier should the need arise.

11 Misuse of CCTV systems

The misuse of CCTV system could constitute a criminal offence.

Any member of staff who breaches this policy may be subject to disciplinary action.

12 Complaints Relating to this Policy

Any complaints relating to this policy or to the CCTV system operated by the Charity should be made in accordance with the FPCA Complaints Policy.

13 CCTV IMPACT ASSESSMENT

Document Version:	V1.2
Date Created:	14/1/26
Author:	Karen Starr
Ratified By:	
Date Ratified:	
Next Review Date:	
Organisation Name:	Florence Park Community Association
Designated Data Protection Officer:	

13.1 Who will be captured on CCTV ?

Anyone in or around the premises, during the entire 24-hour period.

13.2 What personal data will be collected ?

Images of persons in or around the premises. There is an option to retain associated audio.

13.3 What are the purposes for operating the CCTV system?

FPCC has been subject to many break-ins over the years, mostly due to the presence of a bar on the premises. We are often asked by the police for CCTV. We need to be able to monitor unsocial behaviour, theft, vandalism etc.

13.4 What is the lawful basis for operating the CCTV system?

Crime Prevention, Security, Property Protection

13.5 Who is/are the named person(s) responsible for the operation of the system?

Karen Starr (Centre Manager) on Florenceparkcommunitycentre@gmail.com
Richard Henderson (Enter-At) on richard@enter-at.co.uk

There is a requirement for a further member of the Management Committee to cover the Centre Manager's absence.

13.6 Describe the CCTV system, including:

- how this has been chosen to ensure that clear images are produced so that the images can be used for the purpose for which they are obtained;
- siting of the cameras and why such locations were chosen;
- how cameras have been sited to avoid capturing images which are not necessary for the purposes of the CCTV system;
- where signs notifying individuals that CCTV is in operation are located and why those locations were chosen; and
- whether the system enables third party data to be redacted, for example via blurring of details of third-party individuals.

The cameras are in each room, hall way and around the centre in an attempt not to leave blind spots. There are no cameras in the toilet block. Signs are in each room and around the exterior of the building. The cameras do not record certain activities such as Acupuncture etc. Where necessary, e.g. when a room is used as a changing room, the images are blocked out.

13.7 Set out the details of any sharing with third parties, including processors:

Our CCTV/Wifi Consultant (Enter-At) is the only external party with the ability to access the footage.

13.8 Set out the retention period of any recordings, including why those periods have been chosen:

14-30 days. It is on a loop

13.9 Set out the security measures in place to ensure that recordings are captured and stored securely:

The recordings are stored on a hard drive which is in a locked cabinet. Only the Consultant and the Centre manager can access the hard drive.

13.10 What are the risks to the rights and freedoms of individuals who may be captured on the CCTV recordings?

- Undesignated individuals could gain access to the CCTV images for nefarious purposes
- Images could be viewed by staff with credited access, for personal gain

13.11 What measures are in place to address the risks identified?

- Only 2 designated individuals and the IT Consultancy are issued with passwords to the system.
- The CCTV PC has a screen lock password.
- The Chair, FPCA will review the CCTV logs on a regular basis to ensure there has been no misuse of data

13.12 Have staff and visitors where appropriate been consulted as to the use of the CCTV system? If so, what views were expressed and how have these been accounted for?

All groups and ad hoc hirers are informed. Where they have any worries about privacy, we can suspend recording.

13.13 When will this privacy impact assessment next be reviewed?

31/08/2027

This CCTV Impact Assessment was approved by the data protection officer.

Name of D.P.O: Adam W_____

Date of Approval: 8 December 2025_____