

Freedom Centre

CCTV Policy

Lead responsibility for policy	Michael Jenkins - DPO Date: June 2021
Approved (Trustee)	Date:

Definitions

- a) Building refers to any building that is part of The Freedom Centre, Netherton Road, Gosport, Hampshire.
- b) The Church refers to Brockhurst Baptist Church who manage The Freedom Centre
- c) Trustees refers to the Trustees of The Church

1.1 The Freedom Centre uses closed circuit television (CCTV) images for the prevention, identification and reduction of crime and to monitor the buildings in order to provide a safe and secure environment for staff and visitors, and to prevent the loss or damage to property.

1.2 CCTV surveillance at The Freedom Centre is intended for the purposes of:

- protecting the buildings and assets, both when in use and vacant;
- promoting the health and safety of staff and visitors;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the Police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the building's rules are respected so that it can be properly managed.

1.3 The system comprises of a number of 8 fixed cameras, 7 external and 1 internal.

1.4 The CCTV system is owned and operated by The Church who run the Building and the deployment of which is determined by the Trustees. The CCTV is a standalone system.

1.5 The CCTV is typically not monitored but can be from the main office by the DPO.

1.6 The CCTV Scheme is registered with the Information Commissioner under the terms of the Data Protection Act. This policy outlines the use of CCTV and how it complies with the Act.

1.7 All authorised operators with access to images are aware of the procedures that need to be followed when accessing the recorded images. Operator(s) are trained in their responsibilities under the CCTV Code of Practice. All operators and Trustees are aware of the restrictions in relation to access to, and disclosure of, recorded images.

1.8 The Church complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use.

1.9 The use of the CCTV system will be conducted in a professional, ethical and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy e.g. CCTV will not be used for monitoring employee performance.

1.10 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by The Church, including the provisions set down in equality and other educational and related legislation.

2.0 Justification for Use of CCTV

2.1 The use of CCTV to control the perimeter of The Building for security purposes has been deemed to be justified by The Trustees. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation or of antisocial behaviour.

2.2 CCTV systems will not be used to monitor normal activity in building.

2.3 In other areas of the building where CCTV has been installed, The Trustees have demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues.

3.0 Data Protection Impact Assessments

3.1 Where new CCTV systems or cameras are to be installed, The Church will carry out a full Data Protection Impact Assessment identifying risks related to the installation and ensuring full compliance with data protection legislation. This may involve the need for consultation with staff, and other building users.

3.2 Where existing CCTV systems are in operation as of June 2021, The Church will endeavour to carry out a full Data Protection Impact Assessment on any upgrade or replacement of the system.

4.0 Location of Cameras

4.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.

4.2 The Church will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act and will make every effort to position cameras so that their coverage is restricted to the Freedom Centre premises, which may include outdoor areas.

4.3 Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. The Church has endeavoured to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals.

4.4 Cameras placed so as to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

4.5 CCTV Video Monitoring and Recording of Public Areas may take place for the following purposes:

- ***Protection of buildings and property:*** The building's perimeter, site entrances and exits, specific indoor spaces where it can be suitably justified.
- ***Video Patrol of Public Areas:*** Parking areas, Main entrance/exit gates
- ***Criminal Investigations (carried out by police):*** Robbery, burglary and theft surveillance

5.0 Covert Surveillance

5.1 The Church will not engage in covert surveillance.

6.0 Notification

6.1 A copy of this CCTV Policy will be provided on request to staff and visitors and will be made available on the Freedom Centre website www.freedomgosport.com.

6.2 The location of CCTV cameras will also be indicated and adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation.

6.3 Adequate signage will also be prominently displayed at the entrance to the property. Signage shall include the name and contact details of the data controller as well as the specific purpose(s) for which the CCTV camera is in place in each location.

Appropriate locations for signage will include:

- at entrances to premises i.e. external doors, gates
- at or close to each internal camera

7.0 Storage and Retention

7.1 The images captured by the CCTV system will be retained for a maximum of 30 days, except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

7.2 The images/recordings will be stored in a secure environment with a log of access kept.

7.3 Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the DPO. The DPO may delegate the administration of the CCTV System to another Trustee.

7.4 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

7.5 Files/DVDs will be stored in a secure environment with a log of access to data kept. Access will be restricted to authorised personnel.

8.0 Access

8.1 Recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to footage will be maintained.

8.2 Access to the CCTV system and stored images will be restricted to authorised personnel only.

8.3 When accessing images two authorised persons must be present. A written record of access will be made. Records of access will be kept.

8.4 A record of the date of any disclosure request along with details of who the information has been provided to (the name of the person and the organisation they represent), why they required it and how the request was dealt with will be made and kept, in case of challenge.

8.5 Data will be provided to those requests authorised in a permanent format where possible. If this is not possible the data subject will be offered the opportunity to view the footage.

8.6 In relevant circumstances, CCTV footage may be accessed:

- By the police where The Church (or its agents) are required by law to make a report regarding the commission of a suspected crime; or
- Following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on Freedom Centre property, or
- To the HSE and/or any other statutory body charged with child safeguarding; or
- To data subjects (or their legal representatives), pursuant to a Subject Access Request or

- To individuals (or their legal representatives) subject to a court order.
- To The Church's insurance company where the insurance company requires same in order to pursue a claim for damage done to the insured property.

9.0 Subject Access Requests (SAR)

- 9.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.
- 9.2 Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.
- 9.3 The Church will respond to requests within 30 calendar days of receiving the request in line with our right of access policy.
- 9.4 The Church reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.
- 9.5 A record of the date of the disclosure along with details of who the information has been provided to (the name of the person and the organisation they represent) and why they required it will be made.
- 9.6 In giving a person a copy of their data, The Church will provide a still/series of still pictures, a disk with relevant images. However, other images of other individuals will be obscured before the data is released.
- 9.7 Where footage contains images relating to 3rd parties, The Church will take appropriate steps to mask and protect the identities of those individuals.

10.0 Complaints

10.1 Complaints and enquiries about the operation of CCTV within the Freedom Centre should be directed to the DPO in the first instance.

11.0 Training

11.1 Persons authorised to access the CCTV system will be trained to comply with this policy. Those persons will understand that all information relating to the CCTV images must be handled securely.

11.2 Persons will receive appropriate training to enable them to identify and handle different requests according to regulations.

11.3 Any misuse of surveillance system information will lead to disciplinary proceedings.

12.0 Responsibilities

12.1 The DPO (or nominated deputy) will:

- Ensure that the use of CCTV systems is implemented in accordance with the policy set down by The Freedom Centre
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within building
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- Ensure that the CCTV monitoring is consistent with the highest standards and protections
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- Give consideration to both feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the building and be mindful that no such infringement is likely to take place
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring footage are stored in a secure place with access by authorised personnel only
- Ensure that images recorded on DVDs/digital recordings are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil).
- Ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas