

Lincolnshire YMCA Ltd

Policy Document

CCTV

Owned by:	Corporate Services Director
Reviewed by:	Corporate Services Director
Date Approved:	07.07.25
Review Date:	07.07.28

1. INTRODUCTION

1.1 Lincolnshire YMCA uses closed circuit television ('CCTV') within its premises. for the purpose of:

- Crime prevention (ie deterrence) and detection,
- Staff, client and public safety,
- To enable staff with access to recordings to activate our procedure for dealing with crime and other unwanted behaviour

We do not allow the use of CCTV for any other purpose.

1.2 Lincolnshire YMCA is legally responsible for the CCTV system under UK General Data Protection Regulation (UK GDPR)/Data Protection Act 2018. ('the Act'). References to 'we' and 'our' in this Policy are references to Lincolnshire YMCA. This Policy applies to any employee or other member of staff (including contractors, temporary staff, trustees and volunteers) who has access to, responsibility for, or may otherwise use, the CCTV system.

1.3 We must comply with the requirements of the Act whenever our CCTV system views or records information that is 'personal data'. The term 'personal data' is defined by the Act to mean data which relates to a living individual who can be identified from such data or from such data and other information which is in our possession, or likely to come into our possession. Therefore, our use of CCTV will be subject to the Act if:

- the CCTV images are clear enough to identify particular individuals and what they are doing, or captures other information relating to individuals that might identify them, eg vehicle registration numbers;
- the images tell us something about particular individuals;
- the images can be used to take action in relation to an individual (eg by handing them over to the police in order to investigate a crime).

1.4 The Act applies to the 'processing' of personal data contained within the CCTV images. The term 'processing' is defined to include the viewing and recording of images, as well as deleting, holding, retaining, disclosing and destroying the images. For example, when we disclose CCTV images to a third party, that disclosure is a processing activity that must comply with the Act. Virtually anything we do with the images will involve processing of some kind. Whenever you see the words 'process', 'processed' or 'processing' in this Policy you should remember the wide definition set out in this paragraph.

2. YOUR RESPONSIBILITIES

2.1 In this Policy, references to our staff include all employees, workers, contractors, temporary workers, agents and trustees of Lincolnshire YMCA.

2.2 As our CCTV system will be processing personal data (as described above), we have an obligation to ensure that its operation and use complies with the requirements of the Act. All staff who are responsible for implementing, managing, operating or using the CCTV system must help us to comply with the Act by:

- only using the CCTV system as authorised and in accordance with this Policy; ensuring that monitoring is carried out in a way that reassures and notifies individuals who are being monitored;
- only using the CCTV system for the limited purposes described in paragraph of this Policy and for no other purpose.

2.3 If monitoring is carried out properly and lawfully, this will minimise the risk of us being exposed to reputational and other risks associated with data breaches and regulatory action.

2.4 Failure to comply with this Policy could be regarded as a disciplinary offence which could result in dismissal. Gross negligent or deliberate breaches could even result in criminal liability for you personally.

3. INITIAL ASSESSMENT

3.1 Before installing the CCTV system, we carried out a privacy impact assessment to identify the potential privacy risks in relation to our use of CCTV and our approach compliance with the Act. Our assessment concluded as follows:

- The purposes for the CCTV system are those specified in paragraph 1.1 of this Policy;
- Use of the CCTV System benefits us because it enables our staff to work in an environment where they are protected from crime and other unwanted behaviour, and enables our service users to enjoy the same privilege.
- Where crime or other unwanted behaviour does take place, our CCTV Systems critical to identifying perpetrators and assisting in successful prosecutions or civil action where appropriate.
- The personal data processed by the CCTV system are: images of our staff and service users and car parks.
- The legal basis for the processing of personal data by the CCTV system is to enable us to discharge our duty to care for the health and safety of our staff, and our common law duty of care to our service users and members of the public. The justification for processing personal data is set out in paragraph 3 of Schedule 2 of the Act;
- The members of staff who will be responsible for the management and operation of the CCTV system are: departmental and senior

managers.

- Support from third-party service providers will be required in relation to the following: (*specify, eg editing CCTV images, maintaining the CCTV equipment*).

3.2 Any questions relating to the assessment should be directed to the Chief Executive.

4. SITING THE CAMERAS

4.1 The position of the CCTV cameras is critical to ensuring our compliance with the Act. Relevant staff must apply the following principles whenever you are siting cameras:

- cameras should be restricted to monitor only those areas which are intended to be monitored;
- cameras should not be used to monitor any adjoining areas which are not intended to be covered by the system (such as gardens, private dwellings, changing rooms or toilet areas where there is an expectation of privacy);
- where cameras are adjustable, they should be restricted so that they cannot be adjusted to overlook areas outside the CCTV monitored site;
- cameras should be positioned to record images which are relevant to the purposes for which we run the system;
- cameras must be sited to ensure they can produce images of the right quality. Consider the technical capabilities of the camera, the environmental factors, the lighting and the size of the area to be viewed by the camera;
- cameras should be sited so that they are secure and protected from vandalism or other damage.

5. SIGNAGE

5.1 We are required to notify individuals if they are in an area where CCTV surveillance is being carried out. Typically, this is achieved through the use of prominent signs which are located at the start of the CCTV zone, with reminder notices placed at various locations inside the monitored zone.

5.2 The signs should alert individuals that they are entering a CCTV monitored zone in a legible and clear way. Ordinarily, signs should read as follows:
“Warning: CCTV images are being recorded for the purpose of crime prevention and detection and public safety. This system is controlled by Lincolnshire YMCA.”

5.3 We notify our staff that they may be recorded by CCTV through this Policy. The limited exception to this is covert monitoring, see paragraph 10.

6. STORING IMAGES

- 6.1 We must maintain the integrity of all images whilst they remain in our possession. This is necessary to ensure that the evidentiary value of those images is protected (ie so they can be used as evidence in court).
- 6.2 CCTV images must be stored on a secure medium and in a secure place to which access is controlled. We have an obligation to keep CCTV images secure at all times so as to prevent unauthorised viewing or disclosure. To ensure that we meet our security obligations you must ensure that:
- access to the images is restricted to authorised staff only;
 - disclosure of images (where permitted) is undertaken using a secure method of transmission or delivery (so as to minimise the risk of images getting lost in transit or being intercepted);
 - control rooms and areas where images are stored are kept secure at all times and locked when unoccupied;
 - you undertake all necessary training when we make this available to you;
 - Images should be retained for no longer than the retention periods specified in para- graph 14.

7. VIEWING IMAGES

- 7.1 As a general rule, CCTV images should only be viewed and accessed by authorised personnel. Other personnel and third parties (such as the police) should only be allowed to view the images where it is necessary in connection with the purposes set out in paragraph 1.1 above or as otherwise permitted in this Policy. The mere act of viewing is a processing activity that is subject to the Act.
- 7.2 The following rules apply to the viewing of CCTV images:
- the viewing of live images on monitors should be restricted to the operator of the CCTV system;
 - recorded images should be viewed in a restricted area (eg a designated secure office). Access to this area should be restricted whilst the viewing is taking place;
 - where the CCTV system records images from areas that individuals would expect to be private (eg changing rooms or toilets), these images should only be viewed by restricted and authorised employees.
- 7.3 Where it is necessary to allow other personnel, or a third party (such as the police) to view the CCTV images, a record should be made of the following:
- the date and time of the viewing;
 - the name of the person viewing the images and the organisation he or

- she represents;
- the reason for the viewing;
- the basis upon which the viewing was allowed;
- the outcome, if any, of the viewing.

- 7.4 In circumstances where a vulnerable person is reported missing, designated staff may be granted expedited access to relevant CCTV footage to assist in locating the individual and ensuring their safety.

Access will be strictly limited to those with appropriate safeguarding responsibilities or designated security personnel and will be granted in accordance with data protection legislation and internal safeguarding procedures. All access must be logged and authorised by a senior manager or safeguarding officer.

CCTV footage may be reviewed to:

- Determine the last known whereabouts of the missing person.
- Identify any persons seen accompanying or approaching the individual.
- Assist the police or emergency services in real-time or as part of an investigation.

8. DISCLOSURE OF IMAGES

- 8.1 In certain circumstances it may be necessary to disclose the CCTV images to a third party, such as the police. The disclosure is likely to involve the physical delivery of the images or copies to the third party (eg on a USB or by email). Disclosures to third parties must be consistent with the purposes set out in paragraph 1.1 and the provisions of this Policy and comply with GDPR.

- 8.2 Disclosures are permitted in the following circumstances:

- crime prevention purposes - where the disclosure is requested for the purpose of preventing or detecting crime, apprehending or prosecuting offenders, or assessing or collecting tax (the crime and taxation purposes). The third party making the request must:
- justify its request for the CCTV images;
- confirm that a failure to make the disclosure would be likely to prejudice any of the crime or taxation purposes;
- put their request in writing, signed by a senior police officer.

Statutory or other legal obligation - the disclosure of the images may be required under statute (other than under the Act) or may otherwise be legally

required (eg under a court order). In this situation:

- we must disclose the CCTV images if the statutory provision imposes upon us a **mandatory** duty to disclose or a court order requires disclosure;
- we can choose whether to disclose the CCTV images if the statutory provision imposes upon us a **discretion** as to whether or not to disclose.

8.3 In limited circumstances it may also be possible to make a disclosure where it is necessary for the purpose of establishing, exercising or defending legal rights, obtaining legal advice or in connection with legal proceedings. This covers not just our legal rights but also those of third parties. A record should be kept of all requests for disclosure of CCTV images, together with any reasons for refusing a request. If a disclosure is approved and CCTV images are disclosed to a third party, a record should be made of the following:

- the date and time of the disclosure;
- the name of the person to whom the disclosure is made and the organisation he or she represents;
- the reason for the disclosure and the images disclosed;
- the basis upon which the disclosure was made;
- the location where the images are to be kept;
- the outcome, if any, of the disclosure;
- the date and time the images were returned (if applicable);
- if the disclosure is to the police, record any crime incident number to which the images relate and ask the collecting police office to sign for the images when they are handed over.

Where a decision has been made to disclose CCTV images, the disclosure must be made securely so that the images are received by the intended recipient.

All disclosures of CCTV images must be approved by the Chief Executive unless this is not reasonably practicable (because of an emergency and they are unavailable, in which case disclosure must be authorised by the next most senior member of staff available.)

9. SUBJECT ACCESS REQUESTS

9.1 Individuals have a right to access personal data which we process about them, which includes (in most cases) CCTV images of them. If you receive a request from an individual asking to see CCTV images involving him or her or otherwise mentioning access to personal data, you should refer the request promptly to the Data Protection Officer (Corporate Services Director). There are timescales within which a request must be handled, therefore you should act quickly.

If the CCTV images of the data subject include the images of other identifiable

individuals, it may be necessary to obscure the images of the other individuals if providing their images to the data subject would involve an unfair intrusion into their privacy or cause them unwarranted harm or distress. Where there is no such intrusion or harm, then it may not be necessary to obscure the other individuals' identities.

- 9.2 No data should be released without the express consent of the Data Protection Officer (Corporate Services Director).

10. RETENTION PERIOD FOR IMAGES

- 10.1 The Act prevents us from keeping CCTV images for longer than necessary for the purposes set out in paragraph 1.1 above. Generally, we will retain CCTV recordings for no longer than 31 days.
- 10.2 If there are good reasons for retaining CCTV images for longer than the retention period specified above then this is permitted, as long as the images are deleted as soon as the reason ceases to exist. For example, if there is an ongoing criminal investigation which requires access to the CCTV images, then we should retain them until such time as they are no longer needed.

Once CCTV images are no longer needed or the retention period has expired, they should be securely destroyed or erased.

11. NOTIFICATION

Our entry on the Register of Data Controllers (also known as a 'notification') which is maintained by the Information Commissioner must include the purpose(s) for which the CCTV system will be used as well as a description of the disclosures that may be made and other relevant details.

12. PERIODIC REVIEW

The Data Protection Officer will carry out a periodic review of the continued justification for and effectiveness of the CCTV system in operation within our business in fulfilling the purposes in paragraph 1.1 and compliance with this Policy. You will provide all reasonable assistance in the performance of these periodic reviews and, if asked, take all necessary steps to implement any recommendations or changes which result from such reviews.

13. CONTACTS AND RESPONSIBILITIES

- 13.1 If you have any queries about this Policy, please contact the Data Protection Officer. (Corporate Services Director).
- 13.2 We reserve the right to change this Policy from time to time to take into account any relevant changes in law or guidance from the Information

Commissioner, or for other business reasons.

- 13.3 We may carry out checks or audits from time to time to ensure that the requirements of this Policy are being followed.