

P-20 CCTV Policy

Version	Date of change	Changed by	Trustee approval	Notes
1.0	10/12/2024			First draft
1.2	17/04/2025	LMW		Revisions following consultation with various parties
1.3	28/4/2025	LMW	22/4/2025	Approved subject to change as minuted

Purposes

Haxby & Wigginton Youth & Community Association (HWYCA) has installed CCTV cameras at Oaken Grove Community Centre to:

- Deter anti-social behaviour,
- Enhance the safety of visitors, staff, and volunteers,
- Prevent damage to the property.

The use of CCTV is based on legitimate interests under Article 6(1)(f) of the UK GDPR, balancing the security of the premises with the privacy rights of individuals.

Scope

The CCTV cameras are installed at the front of the Community Centre Building, one in the Children's Library pointing towards the main gates and the other in the Adult Library pointing towards the car park, bike shed, and pedestrian access at the rear of the car park.

It is not the intention to capture sensitive data such as vehicle registration numbers and members of the public. The system does not use Automatic Number Plate Recognition (ANPR) technology.

The system will provide twenty-four (24) hours per day and seven (7) days per week recording over the areas mentioned above.

As the cameras are positioned within the building audio will not be recorded or stored.

The use of CCTV cameras is done so in accordance with the Data Protection Act 2017.

Legal Compliance

This policy complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

A Data Protection Impact Assessment (DPIA) has been completed to ensure that the use of CCTV is proportionate, necessary, and minimises risks to individuals' rights and freedoms.

Signage/Notification

Signs are clearly displayed:

- Around the front of the building, visible outside the fences,
- At the main entrance foyer.

Each sign includes:

- Notification that CCTV is in operation,
- The identity of HWYCA,
- Contact details for further information.

Retention Period And Backup

Images of the CCTV system will be recorded and kept for a period of 30 days via the Reolink Cloud Storage Location. As such images will not be constantly viewed. Only images which have been downloaded relating to a crime or incident will be potentially retained for longer. The images will be automatically deleted after 30 days by Reolink Cloud.

Reolink Terms of Use can be found here: <https://cloud.reolink.com/terms-of-use/>

Reolink Privacy Policy can be found here: <https://reolink.com/privacy-policy/>

Reolink Terms and Conditions are available here: <https://reolink.com/terms-conditions/>

Any footage that shows a crime will be kept as long as it is needed to confirm if criminal proceedings will be undertaken.

Images that are stored on, or transferred on to, removable media such as a USB flash drive are erased or destroyed or deleted once the purpose of the recording is no longer relevant. Where a law enforcement agency is investigating a crime, images may need to be retained for a longer period. Downloaded footage will be kept securely, either on a USB flash drive locked in a secure location within the office, or on a password protected computer in the office.

Maintenance checks of the equipment are undertaken on a regular basis to ensure it is working properly and that the media is producing high quality images. These will comprise of visual checks of the two cameras to ensure they are operating correctly, and will take place quarterly as part of the Health & Safety building checks. Checks to ensure the footage captured on the Reolink Cloud will also be undertaken by authorised members of staff.

Security Measures

As per Section 31 of the Data Protection Act:

- Only authorised personnel will have access to the CCTV Cloud Storage, and this will be limited to named members of key staff and a maximum of two Trustees.
- At least one member of staff viewing the footage must be DBS checked.
- An audit trail has been implemented to monitor staff access to the footage.
- Password Protection will be in place to manage staff access to stored footage.
- Footage must only be accessed by two authorised members of staff or trustees, never by an individual member of staff or Board of Trustees.
- Quarterly audits of system security and access processes will take place.
- The Realink website is password protected.
- The images will not be accessed or viewed via a mobile phone.
- Images will only be reviewed on the desktop computer located in the Oaken Grove Community Centre office.

Disclosure Of CCTV Footage

HWYCA will not disclose the CCTV footage to any unauthorised third party.

Surveillance information and images may be disclosed to relevant law enforcement agencies (e.g. Police).

Disclosure of images to other third parties will only be made in accordance with the purposes for which the system is used and will be limited to:

- The police and other law enforcement agencies, where the images recorded could assist in the prevention or detection of a crime or the identification and prosecution of an offender or the identification of a victim or witness.
- Prosecution agencies, such as the Crown Prosecution Service.
- Relevant legal representatives.

- The centre managers when involved in disciplinary and performance management processes.
- Individuals whose images have been recorded and retained (unless disclosure would prejudice the prevention or detection of crime or the apprehension or prosecution of offenders).

Images from the CCTV system will not be shared on the internet.

Information about identifiable individuals will not be disclosed to the media.

A minimum of two of the authorised personnel are required to permit the disclosure of images to external third parties such as law enforcement agencies, and they must both be in agreement before disclosure is approved. Authorised personnel will be limited to named members of key staff and a maximum of two Trustees.

All requests for disclosure and access to images will be documented, including the date of the disclosure, to whom the images have been provided and the reasons why they are required. If disclosure is denied, the reason will be recorded.

Request For Access Of CCTV Footage

Subject to section 37 of the Data Protection Act 2017, individuals whose images are recorded have a right to view the CCTV images/footage about themselves and to be provided with a copy to them. HWYCA reserves the right to charge a fee of £10.00 for the supply of the images requested.

If there are other identifiable people in the footage, HWYCA will look at options to protect those people's privacy, for instance by masking other individuals on the footage. In this case, the images of third parties may need to be obscured if it would otherwise involve an unfair intrusion into their privacy.

Note: As per section 37(6), if HWYCA refuses to take action on the request of a data subject (individual), it shall, within one month of the receipt of the request, inform the data subject in writing of the reason for the refusal and on the possibility of lodging a complaint with the Commissioner.

Process for CCTV Subject Access Requests

Personal information can be requested under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Requesting information is classed as a Subject Access Request (SAR). Individuals who wish to make a SAR, can make a request either in writing or verbally. HWYCA reserves the right to charge a fee of £10.00 for the processing of SARs if a request is manifestly unfounded, excessive or repetitive.

In order for HWYCA to ensure that information is only released to the appropriate individuals, identification checks may be needed. It may, therefore, speed up an individual's request if they

are able to provide proof of identification, such as a driver's licence or passport.

Individuals can request footage of themselves only, and when doing so must confirm the following details:

- The place where the incident occurred;
- The date when the incident occurred;
- The time when the incident occurred.

SARs need to be sent to the Community Services Manager at Oaken Grove Community via email at info@hwyca.co.uk, or telephone on: 01904 769176.

HWYCA has 30 days to respond to a SAR from the date of receipt.

SARs will be logged using a spreadsheet which is password protected and only accessed by authorised members of staff.

Procedures To Handle Incidents

Incidents captured by CCTV will be reported to the Police, or relevant party as appropriate.

Incidents involving young people will be referred to the HWYCA Youth Manager, and action will be taken where appropriate based on the Safeguarding and Behaviour Policies. If the young person is not recognised the matter will be referred to the Police as necessary.

Policy Breaches

If a member of staff breaches this policy they will be subject to P-12 Disciplinary Process.

Policy Review

This policy will be reviewed annually or in response to:

- Changes in legislation,
- Technological updates,
- Operational changes at the Centre.