

The Federation of Kintore Way Nursery School & Children's Centre & The Grove Nursery School

CCTV Policy

Introduction

The federation recognises that CCTV systems can be privacy intrusive.

For this reason, the Federation has carried out data protection impact assessments with a view to evaluating whether the CCTV systems in place are a necessary and proportionate means of achieving the legitimate objectives set out below.

The results of the data protection impact assessments has informed the Federation's use of CCTV and the contents of this policy.

Review of this policy shall be repeated regularly and whenever new equipment is introduced, a review will be conducted and a risk assessment put in place. We aim to conduct reviews no later than every two years.

Objectives

The purpose of the CCTV system is to assist the Federation in reaching these objectives:

- (a) To protect pupils, staff and visitors against harm to their person and/or property.
- (b) To increase a sense of personal safety and reduce the fear of crime.
- (c) To protect the school buildings and assets.
- (d) To support the police in preventing and detecting crime.
- (e) To assist in identifying, apprehending and prosecuting offenders.
- (f) To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence.
- (g) To assist in managing each school.

Purpose of this Policy

The purpose of this Policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at each school. The CCTV system used by the federation comprises of:

Kintore Way:

CAMERA TYPE	LOCATION	SOUND	RECORDING CAPACITY	SWIVEL / FIXED
HIKVISION	Outside the Main Front Entrance Door	N	Y	F
HIKVISION	Inside the Main Front Entrance Door facing pram space	N	Y	F
HIKVISION	Inside the Foyer facing the main reception desk	N	Y	F

HIKVISION	Facing the Nature Garden Gate towards the road	N	Y	F
HIKVISION	Showing the alley way towards the parent exit, facing the exit gate inside the school	N	Y	F

Grove:

CAMERA TYPE	LOCATION	SOUND	RECORDING CAPACITY	SWIVEL / FIXED
HIK DS-2CE56D8T	Outside the Main Front Entrance Door	N	Y	F
HIK DS-2CE56D8T	Outside on the corner of the front of the pram shed facing the gates to the pram shed	N	Y	F
HIK DS-2CE56D8T	Outside facing playground	N	Y	F
HIK DS-2CE56D8T	Outside the kitchen facing refuse bins	N	Y	F
HIK DS-2CD2T25FWD	Pram Shed	N	Y	F
HIK DS-2CD2T25FWD	Pram Shed	N	Y	F

Statement of Intent

Notification has been submitted to the Information Commissioner and the next renewal date has been recorded.

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The Federation will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation on adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the system will give maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on each site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

Recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. In the absence of compelling a need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than one month.

System Management

Access to the CCTV systems and data shall be password protected.

The CCTV systems will be administered and managed by the Premises Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager the systems will be managed by the Federation School Business Manager.

The systems and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Executive Headteacher.

The CCTV systems are designed to be in operation for 24 hours each day, every day of the year, though the Federation does not guarantee that they will be working during these hours.

The System Manager will check and confirm the efficiency of the systems regularly and in particular that the equipment is properly recording and that cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by proving clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned in paragraph 5.3 above, requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists access will be refused.

Details of all visits and visitors will be recorded in a system log book including time/data of access and details of images viewed and the purpose for so doing.

Downloading Captured Data onto other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- (a) Each download media must be identified by a unique mark.
- (b) Before use, each download media must be cleaned of any previous recording.
- (c) The System Manager will register the date and time of download media insertion, including its reference.
- (d) Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence

store. If a download media is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed and signed by the System Manager, then dated and returned to the evidence store.

(e) If download media is archived the reference must be noted.

Images may be viewed by the police for the prevention and detection of crime and by the Systems Manager, his/her replacement and the Executive Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any download media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the relevant school within the federation, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The federation also retains the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media this will be produced from the secure evidence store, complete in its sealed bag.

The police may require the relevant school within the Federation to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors or parents) to view or release images will be referred to the Federation's Data Protection Officer and a decision made by a senior leader of the Federation in consultation with the Federation's Data Protection Officer.

Complaints about the use of CCTV

Any complaints in relation to either school's CCTV system should be addressed to the Executive Headteacher.

Request for Access by the Data Subject

The Data Protection Act provides Data Subjects – those whose image has been captured by the CCTV system and can be identified – with a right to data held about themselves, including those obtained by CCTV. Requests for such data should be made to:

Data Protection Officer: Craig Stilwell
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

Public Information

Copies of this policy will be available to the public from each school's office.

The Federation of Kintore Way Nursery School & Children's Centre & The Grove Nursery School

Policy Name
CCTV Policy

Adopted and signed on behalf of The Federation of Kintore Way Nursery School & Children's Centre & The Grove Nursery School by the Governing Body at the meeting on

14th December 2020

Name of Governing Body Representative

Teresa Ali

Signature of Governing Body Representative



Date signed 14th December 2020

Date to be reviewed: As and when changes are made