CCTV

STATUTORY / NON-STATUTORY	**NON-STATUTORY**
MEMBER OF STAFF RESPONSIBLE	**AHT (HLo)**
DATE APPROVED BY Head/SLT	**March 2021**
GOVERNING BODY OR COMMITTEE RESPONSIBLE	**GP**
DATE OF FULL GOVERNING BODY APPROVAL	**March 2021**
REVISION DUE DATE	**March 2023**

Contents

Introduction

This Policy sets out the appropriate actions and responsibilities, which must be followed to comply with the legislation and guidance in respect of CCTV surveillance systems managed by the School :

- To inform all who enter School property that CCTV is in use.
- To ensure images from CCTV are stored securely and controlled by authorised personnel.
- To maintain all CCTV equipment in good working order.
- To provide retention of images within the stated purpose and timeframes only.
- To state the manner and means of destroying stored images.
- To prevent access by unauthorised individuals or third parties.

The purpose of this Policy is to ensure that Noadswood School uses CCTV responsibly and within effective safeguards. The intention is :

- To create a safe environment for pupils, staff, contractors and visitors.
- To protect property belonging to pupils, staff, contractors and visitors.
- To protect the property, facilities and equipment.
- To provide evidence in support of any internal or external enquiry, disciplinary proceedings or prosecution, especially if associated with the security of the School premises and members of the School community; criminal activity committed on School property, or the misuse of School property, facilities or equipment.

Following is a list of example incidences that would warrant review of the CCTV system:

- Vandalism
- Intimidation
- Bullying
- Theft
- Missing Pupil
- Near Miss Incident
- Accident

CCTV will not be reviewed for the purposes of staff or pupil punctuality, or monitoring staff or pupils working.

Cameras are located internally and externally throughout the School. Signage is located at the external entrances / exits to the School property.

Cameras transmit images to a dedicated school CCTV server which has restricted access (ICT Department only) and is located in the IT Server Room which has restricted access (ICT Department only). Other members of staff or contractors requiring access to the IT Server Room will be escorted by a member of the ICT Department. Upon request, Site Team staff may, on occasion, be permitted non-escorted access to the IT Server Room.

Noadswood School has completed a CCTV Impact Assessment.

Legal Framework

The system shall be used in accordance with all relevant legislation and guidance:

- Data Protection Act 1988
- Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 200
- General Data Protection Regulation 2016/679 (GDPR)
- Information Commissioners Office CCTV Code of Practice

Related Noadswood School Polices are:

- Data Protection Policy
- Freedom of Information Policy
- GDPR

CCTV Locations

Prior to any CCTV installation, the Data Protection Officer, in conjunction with the Headteacher, will ensure that the installation complies with relevant legislation. The School does not use covert cameras. All CCTV locations are visible to staff, pupils, contractors, visitors and members of the public. Signage has been erected at the Main Entrances / Exits to the School property to notify all those who enter that they are entering an area that is covered by CCTV.

Responsibilities

Noadswood School's CCTV System is registered with the Information Commissioners Office, under registration number Z3053082. The registration is renewed annually in February.

The system is operated by Noadswood School and is in use all year round. The Governing Body and Headteacher have overall responsibility for the implementation and use of the system and have delegated responsibility to the Data Protection Officer.

The Premises Manager is responsible for ensuring the equipment is maintained in suitable condition and good working order.

Live images and recorded data stored on the CCTV Server can be viewed by Authorised Users only.

The High-Level Authorised Users (to include toilet areas) of the system are:

- Headteacher
- Deputy Headteacher (Data Protection Officer)
- Designated Safeguarding Lead (DSL)

The Authorised Users of the system are:

- Senior Leadership Team
- Di Ward - House Leadership Representative

High Level Authorised Users have access to the entire system, with administrative rights. Authorised Users of the system are granted a lower level of access to the system.

Operation of the system is restricted to those identified above, although Authorised Users can permit supervised viewing by other members of staff for the purposes of identification of individuals or incidents only.

Authorised Users of the CCTV system have the following responsibilities:

- To uphold the arrangements of this Policy.
- To handle images and data securely and responsibly, within the aims of this Policy.
- To be aware that they could be committing a criminal offence if they misuse CCTV images.
- To uphold the recorded procedure for Subject Access Requests.
- To report any breach to the Data Protection Officer.
- To attend training / refresher sessions as required.

Access to the system is restricted to the Authorised Users only. The system has been set to log Authorised Users directly into their permitted access level only.

Authorised Users may view live data from any camera within their permitted access level during their normal working hours.

In response to an ongoing event, Authorised Users may review recently recorded footage (material is stored securely for a maximum 12 days) to ascertain any facts necessary to respond to an incident.

Copies of live or stored data are not generally permitted. If this is necessary, the following procedures for Storage, Viewing and Processing of Stored Data must be followed.

An Internal Viewing Record will be completed by the Authorised Users each time the system is accessed.

Incident Management

If criminal or suspicious activity of a serious nature is observed, then the School will immediately inform the Police. Once an incident is reported to the Police, it will be dealt with in accordance with Police procedures. All other incidents will be logged and dealt with by the relevant authorities or internally within the School as appropriate.

If an incident is reported, or damage is identified within the School property and thought to have been caused by a pupil, this will be reported to a member of the House Leaders Guidance team for investigation.

Storage, Viewing and Processing of Stored Data

The following procedures concerning the use and retention of stored data will be followed in order to provide an acceptable level of security and accountability, and to ensure the acceptance of recordings in support of criminal proceedings:

- Stored data from the CCTV cameras is retained on the dedicated CCTV Server for a maximum of 12 days and is then overwritten.

- The ‘Recycle Bin’ feature has been disabled on the CCTV Server to ensure overwritten data is fully deleted.
- If an incident occurs, and it is thought that the CCTV system will hold some relevant evidence, the Authorised Users are permitted to access the stored data for the purposes of determining the full details of the incident / extent of the damage.
- Access to the CCTV system will be recorded on the Internal Viewing Record.

Access to and Disclosure of Images to Third Parties

Access to, and disclosure of, images is restricted and carefully controlled to ensure privacy of individuals, but also to ensure that the continuity of evidence remains intact should the images be required for evidential purposes.

On no account may live or stored data be viewed by any unauthorised person.

Staff will be informed that any misuse or unauthorised access of live or stored data will be considered as a serious disciplinary matter.

Individuals requesting access to view images stored within the CCTV system will be asked to complete a Subject Access Request Form. Any request by a third party to view the stored data must be approved by the Data Protection Officer in consultation with the Headteacher, who will determine together whether disclosure is appropriate and whether there is a duty of care to protect the images of any third parties.

Disclosure requests should be addressed to the Data Protection Officer, Noadswood School, North Road, Dibden Purlieu, Southampton, Hampshire, SO45 4ZF. The School will accept electronic (email) correspondence to the Data Protection Officer at the following email address: dpo@noadswood.hants.sch.uk.

If the request is approved, images will be provided within 30 calendar days of receiving a request. If the request is not approved, contact will be made with the individual to advise the reason(s).

Police / Evidential Access

- Requests for Police Access must be recorded on the Third Party Viewing Record.
- Once a valid Third-Party Viewing Record for Police access has been approved by the Data Protection Officer in conjunction with the Headteacher, an Authorised User will supervise the Police Officer(s) while reviewing the relevant stored data.
- If relevant evidence is identified during viewing, an Authorised User will generate a copy of the relevant part of the stored data.
- If stored data is copied onto a common digital media recording device for use by the Police, an Evidential Data Storage Record will be completed.
- A copy of the stored data along with a copy of the Evidential Data Storage Record will be placed into a sealed envelope and identified using a unique reference number, the Individual Data Storage Record will be completed.
- This will be stored securely with the Data Protection Officer and will be released to the Police against an Officers signature as completion of the Evidential Data Storage Record.
- If the School is asked to retain stored data for evidential purposes, the Data Protection Officer will take possession of and securely store the relevant copied data for as long as is required, which would normally be until one month after the finalisation of any court proceedings. The Individual Data Storage Record will be completed.

- Destruction of copy data stored on common digital media recording device(s) is to be recorded using the Data Destruction Record when no longer required. Discs will be shredded and disposed of confidentially by an approved confidential waste disposal contractor.

Applications from Other Third Parties

- Applications from other outside bodies, for example, the CPS, Courts or Solicitors, to view and / or release stored data will be referred to the Data Protection Officer who, in conjunction with the Headteacher, will determine if satisfactory documentation has been provided to support the request.

System Operation and Maintenance

- The School does not have any permanent live CCTV feeds on site. Review of live and stored data takes place only in the following designated restricted access areas when required:
  - Head Teacher's Office
  - Data Protection Officer's Office
  - House Leaders Guidance Office
  - Senior Leadership Team Offices
- The date and time within the CCTV System is directly linked into the School IT Servers, which take the date and time from the Coordinated Universal Time. The Noadswood ICT department will bi-annually check this functionality and report any faults to the third-party maintenance company.
- Cameras will be checked monthly by the appointed third-party maintenance company to ensure all are fully operational. This is an automated system check that does not require data to be viewed.
- Any faults identified by the third-party maintenance company will be notified to the School for investigation.
- Faults unable to be rectified internally will be reported back to the third-party maintenance company for resolution.
- When on site, the third-party maintenance company will work under the supervision of an Authorised User.
- A Fault Log Form is to be completed to record all faults and remedial actions.

Prime Digital polices are outlined here: http://www.prime-digital.com/faqs/ with Hampshire policies outlined here: https://www.hants.gov.uk/educationandlearning/dataprotection.

Records and Retention

- All access to and activities within the CCTV System, as identified within this Policy, must be recorded on the appropriate Record Form(s).
- All completed Record Forms must be returned to the Data Protection Officer within 24 hours of completion.
- All completed Record Forms will be retained by the Data Protection Officer for a period of two years.
- Monthly Operational Reports are retained by the Premises Manager for a period of two years.

Training

All Authorised Users will receive training and refresher training in the practical use of the CCTV system, and management of live and stored data as required. Records identifying the type of training and the named individuals receiving this training will be retained by the Data Protection officer for a period of two years.

Provision and Sharing of Information

A copy of this Policy will be published on the School's intranet and website and will form part of the New Staff Induction Process.

Complaints Procedure

Any individual who has concerns about the CCTV System or the management of it at Noadswood School is requested to write to the Data Protection Officer, Noadswood School, North Road, Dibden Purlieu, Southampton, Hampshire, SO45 4ZF, outlining their concerns or reason for complaint. The School will accept electronic (email) correspondence to the following email address: dpo@noadswood.hants.sch.uk.

Policy Implementation, Monitor and Review

The Premises Manager has been delegated responsibility from the Governing Body / Headteacher / Data Protection Officer for implementing and monitoring this Policy and will be responsible for reviewing this Policy on a biennial basis, additionally whenever there are relevant changes in legislation or to the working practices of the School.