Salendine Nook High School

CCTV Policy (Non-Statutory)

Date policy written:	**February 2018**
Produced by:	**Mrs Virginia Wood**
Approved by Governing Body:	**Finance, Staffing & General Purposes Committee 15.3.18**
Review date:	**March 2020**

Salendine Nook High School considers that;

- The CCTV scheme can contribute to the security and health and safety of all pupils, staff and visitors.
- The purpose of the CCTV scheme at Salendine Nook High School is to provide monitoring systems that assist with the protection of the property, law enforcement, traffic management, community safety and the reduction of crime and disorder, thereby improving the quality of life for all students, staff and visitors to the school.

The Salendine Nook High School confirms that;

- The CCTV systems at the Salendine Nook High School have been notified to the Information Commissioner.
- The general management of CCTV at the Salendine Nook High School is currently vested with the Director of Finance & Resources.
- The day to day management of the CCTV system is the responsibility of the ICT Manager.
- Owner Operator Data and Controller of the Scheme – Principal, Salendine Nook High School, New Hey Rd. Huddersfield HD3 4GN.
- The School's GDPR (Data protection Policy) is referenced to this policy.

The purpose of this policy is to regulate the use of CCTV (closed circuit televisions) systems at the Salendine Nook High School. This code is based upon the Code of Practice published by the Information Commissioner, which set out the standards that must be met if the requirements of the Data Protection 1998 Act are to be met. Section 37 of the Data Protection Act is shown below.

Section 37 of the Data Protection Act

The Data Protection Act requires that all CCTV installations designed to provide either crime prevention, crime detection or to enhance the safety of people on site, must comply with the requirements of the Act.

These are that:

1. Data must be processed fairly and lawfully.
2. Data can only be obtained for lawful purposes.
3. Data shall be adequate, relevant and not excessive
4. Data shall be accurate and kept up to date.
5. Data shall be kept secure and not be kept for longer than is necessary.
6. Data shall be processed in accordance with the rights of individuals under the Act.
7. Appropriate measures shall be taken to prevent unauthorised or unlawful processing of data against accidental loss, destruction or damage.
8. Personal data will not be transferred to a country outside European Economic Area.

1. Data must be processed fairly & lawfully

Cameras are sited in such a way that they only monitor those spaces which are intended to be covered by the equipment.

Signs are placed so that students, staff and the public are aware that they are entering a zone which is covered by surveillance equipment.

The purpose of the use of CCTV is displayed – "CCTV in operation for your safety and security"

Contact details regarding the CCTV scheme are displayed on all external gates.

2. Data can only be obtained for lawful purposes

Disclosure of images to third parties is permissible only in limited and prescribed circumstances. Examples of third parties are:

- Law enforcement agencies if the recorded image would assist in a specific criminal inquiry
- Prosecution agencies
- Relevant legal representatives
- The media, but only in exceptional circumstances if it is decided that the public's assistance is needed in order to assist in the identification of victim, witness or perpetrator in relation to a criminal incident. Permission must be obtained from the Head Teacher prior to release

Data obtained can only be used for the prevention or detection of criminal activity, or the apprehension and prosecution of offenders.

Access to recorded images is restricted to only those who need to have access to achieve the purpose of using the equipment. This access is documented with the following information:

- The identity of the data subject or third party to whom disclosure was made.
- The date of disclosure.
- The reason for allowing disclosure.
- The extent of the information disclosed.
- The name and signature of the managed or designated member of staff allowing the disclosure.

Approved list of school staff that has access to CCTV footage is available from the Finance & Admin Teams and is included here as Appendix 1.All other staff must make a request to a member of SLT.

If you require the CCTV to then be copied to disc/pen drive all staff must request this from a member of SLT.

In accordance with section 7 of the Data Protection Act 1998 (subject access), any individual who believes that their image has been captured by this scheme is entitled to make a written request to the Data Controller, in this case the Principal. Upon payment of the current fee (£10) and the supply of essential information, a systems search will be conducted and subject to certain conditions, the individual will be allowed access to the personal data held. All subject access requests under this clause should be referred in the first instance to the Principal who will liaise with the Director of Finance & Resources and if agreed will be copied to disc and provided to the requestor within 24 days of the request, if the footage is not collected after 24 days it will be destroyed.

All staff involved in operating the equipment must be able to recognise a request for access to recorded images by data subjects and how such requests are to be dealt with. Data subjects should complete the appropriate section of the CCTV Data Form – see Appendix 2. Individuals, at the time of any subject access request, will be given a description of the type of images recorded and retained and the purpose for which the recording and retention takes place. They should be informed of their rights as provided by the 1998 Act.

Prior to any authorised disclosure, the Principal will need to determine whether the images of another 'Third Party' individual features in the personal data being applied for and whether these third party images are held under a duty of confidence.

If the Principal decides that a subject access request, from an individual, is not to be complied with, the following should be documented.

- The identity of the individual making the request
- The date of the request
- The reason for refusing to supply the images requested
- The name and signature of the person making the decision

3. Data shall be adequate, relevant and not excessive

Cameras are sited so that they do not record more information than is necessary for the purpose for which they were installed.

4. Data shall be accurate and kept up to date.

Any personal information which is recorded and stored must be accurate.

The ICT and Finance Teams will ensure that the accuracy of the system features are checked and if necessary amended or altered.

5. Data shall be kept secure and not be kept longer than is necessary

The Director of Finance & Resources is responsible in conjunction with the ICT Manager for ensuring that:

- Images are retained on a hard disc for a period of 10 days. Copies can be made for investigation purposes, but requests for copies must be made via the Principal and must be returned, for destruction within 24 days to the Director of Finance & Resources.
- All CCTV saved footage will only be kept for a maximum of 24 days. Once the retention period has expired, the images will be erased.
- Checking that the equipment performs properly.
- Ensuring any special features are accurate (e.g. time display).
- Reporting immediately if equipment is faulty or damaged.

6. Data shall be processed in accordance with the rights of individuals under the Act

- They have the right to be provided with a copy of the information held about them.
- They have the right to prevent processing which is likely to cause damage or distress.
- They have rights in relation to decision taking.

7. Appropriate measures shall be taken to prevent unauthorised or unlawful processing of data against accidental loss, destruction or damage.

It is required that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of data and against accidental loss, damage or destruction.

In order to achieve this there is a need to assess any harm that might result from the processing, damage, loss or destruction of this data.

The nature of the data to be processed should be considered and where it contains details of inappropriate/unnecessary material it must be processed with greater care.

8. Personal data will not be transferred to a country outside the European Economic Area.

The Principal places limitations on the ability to transfer personal data to countries and territories outside of the EEA.

Data will not be made available to the public via internet or website.

9. Monitoring Compliance with this Code of Practice

The contact point (Director of Finance & Resources) indicated in the sign should be available to members of the public during normal office hours.

Enquiries should be provided on request with a copy of this code of practice.

The Director of Finance and Resources should undertake regular reviews of the documented procedures to ensure that the provisions of the Code are being complied with.

An internal annual assessment should be undertaken which evaluates the effectiveness of the system.

Details of complaints will be maintained and will be included in an annual report on each CCTV system.

10. General Information

We have CCTV internally:

- 11 cameras located on all ground floor fire call points;
- 7 cameras throughout Salendine Building – main entrance, boys & girls geography/technology corridor toilets, 2 cameras in Isolation;
- 3 cameras in the Sports Hall

We have CCTV externally:

- 2 cameras in the Quad car park

11. System Failure

Should any part of the CCTV system fail for example cameras not working, video viewing not retrievable on any of the systems, this must be reported via e-mail to ICT Helpdesk and to the Director of Finance and Resources.

Appendix 1

STAFF ACCESS RIGHTS

Level	Title	Access
1	ICT Technical Team	Full Access and operational use
1	SLT	Full Access and operational use
2	Finance & Admin Team	Downloading, Copying & Viewing of CCTV footage
3	All HoY's, all AHoY's & all PSU staff	Viewing access only

ALL other staff will need to make a request to a member of SLT

Appendix 2

CCTV DATA FORM

Request to view CCTV – Date	Name	Position	Reason for Request	SLT approval	CCTV Operator	Request to copy CCTV footage – Yes/No	Format	Release of the Footage - Date	Removal of footage - Date	Footage destroyed- date agreed by D of F& R