CCTV Policy

Applicable to:	✓	Astley Community High School
	✓	Seaton Sluice Middle School
	✓	Whytrig Middle School
Approval body:	Resources Committee	

Status:

Statutory policy or document	No
Review frequency	Governing Body to determine
Approval by	Governing Body to determine

Publication:

Statutory requirement to publish on school website	No
Agreed to publish on school website	Yes

Review:

Frequency	**Next Review Due**
Annually	September 2020

Version Control:

Author	**Creation Date**	**Version**	**Status**
Data and Curriculum Services Manager (AD)	22 August 2018	0.1	Initial draft compliant with GDPR, based on WMS policy (December 2014)
Changed by	**Revision Date**		
Business Manager (BW)	21 September 2018	1.0	Final approved version for publication
Business Manager (BW)	1 October 2019	1.1	Authorisation to view images restricted to senior leaders only, on advice from DPO
Business Manager (BW)	21 October 2019	2.0	Final approved version for publication

1 Introduction

1.1 The federation has CCTV surveillance systems (hereby known as "the system") in place on its school sites. Images are monitored and recorded centrally on each site, and will be used in strict accordance with this policy.

1.2 The systems are owned by Seaton Valley Federation, % Astley Community High School, Elsdon Avenue, Seaton Delaval, Northumberland, NE25 0BP.

1.3 The Executive Headteacher is responsible for the operation of the system and for ensuring compliance with this policy and the procedures.

2 General Data Protection Regulation (GDPR)

2.1 CCTV digital images, if they show a recognisable person, are personal data and are covered by the General Data Protection Regulation. This policy is also associated with the federation's Data Protection Policy, the provisions of which should be adhered to at all times.

2.2 The federation's Data Protection Officer and Executive Headteacher are jointly responsible for the federation's Data Protection Policy.

3 The system

3.1 The system comprises fixed position cameras, monitors, digital recorders, and public information signs.

3.2 Cameras will be located at strategic points on the school sites, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focussing on the frontages or rear areas of private accommodation.

3.3 Signs will be prominently placed at strategic points and at entrance and exit points of the school sites to inform staff, students, visitors and members of the public that a CCTV installation is in use.

3.4 Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

4 Purpose of the system

4.1 The systems have been installed with the primary purpose of reducing the threat of crime generally, protecting school premises and helping to ensure the safety of all federation staff, students and visitors, consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- deter those having criminal intent
- assist in the prevention and detection of crime
- facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- facilitate the identification of any activities or events which might warrant disciplinary proceedings being taken against staff or students
- assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken

(including, but not restricted to, use in exclusion decisions in any disciplinary meeting)
- facilitate the movement of vehicles on site
- provide management information relating to employee compliance with contracts of employment

4.2 The system will not be used:

- To provide recorded images for the world-wide-web.
- For any automated decision taking

5 Recording

5.1 Digital recordings are made using digital video recorders. Incidents may be recorded in real time.

5.2 Images will normally be retained for 30 days from the date of recording, and then automatically overwritten. Once a hard drive has reached the end of its use it will be erased prior to disposal.

5.3 All hard drives and recorders shall remain the property of the federation until disposal and destruction.

6 Access to images

6.1 Authorisation to view images will be restricted to members of the Senior Leadership Team (SLT), Student Progress Leaders and Heads of Year. These people may authorise the viewing of images by other members of staff only when it is necessary to fulfil the objectives of the system, for example to identify a person in an image.

6.2 Only the Executive Headteacher or members of the SLT may authorise the viewing of images by non-staff members, and only where it is necessary for the purposes of meeting the objectives of the system.

<u>Access to images by third parties</u>

6.3 Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies, where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media, where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained, unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings
- Emergency services, in connection with the investigation of an accident

<u>Access to images by a subject</u>

6.4 CCTV digital images, if they show a recognisable person, are personal data and are covered by the General Data Protection Regulation. Anyone who believes that they

have been filmed by CCTV is entitled to ask for a copy of the data, subject to exemptions contained in the Regulation. They do not have the right of instant access.

6.5 A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the federation's Data Protection Officer.

6.6 The Data Protection Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the federation's Data Protection Officer.

6.7 The General Data Protection Regulation gives the Data Protection Officer the right to refuse a request for a copy of the data, particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

6.8 If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

7 Complaints

7.1 It is recognised that there may be concerns or complaints about the operation of the system. Complaints regarding the federation's CCTV systems should be made in line with the federation's Complaints Procedure.