	Closed Circuit Television (CCTV) Policy	**Author:**	**Business Manager**
		Approved by:	**Local Governing Body**
		Date:	**21 June 2017**
		Review date:	**June 2018**

1. INTRODUCTION

1.1 The Pingle Academy uses closed circuit television (CCTV) images to monitor behaviour and the academy buildings in order to provide a safe and secure environment for students, staff and visitors, and to prevent the loss or damage to academy property.

1.2 The system consists of 41 dome cameras.

1.3 The system does not have sound recording capability.

1.4 The CCTV system is owned and operated by the academy and its deployment is determined by the Academy's Leadership Team.

1.5 The CCTV system is reactively monitored centrally from the Premises Office by the Premises staff.

1.6 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the academy community.

1.7 The academy's CCTV Scheme is registered through the de Ferrers Trust with the Information Commissioner under the terms of the Data Protection Act 1998. The use of CCTV, and the associated images and any sound recordings, is covered by the Data Protection Act 1998. This policy outlines the academy's use of CCTV and how it complies with the Act.

1.8 All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of, recorded images and sound.

2. STATEMENT OF INTENT

2.1 The academy complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its continued use. The Code of Practice is published at:

http://www.ico.gov.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

2.2 CCTV warning signs will be clearly and prominently placed at all external entrances to the academy, including academy gates if coverage includes outdoor areas. Signs will contain details of the purpose for using CCTV (see appendix B). In areas where CCTV is used, the academy will ensure that there are prominent signs placed at both the entrance of the CCTV zone and within the controlled area.

2.3 The planning and design has endeavoured to ensure that the Scheme 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.

3. SITING THE CAMERAS

3.1 Cameras will be sited so they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that reasonable privacy expectations are not violated. The Academy will ensure that the location of equipment is carefully considered to ensure that images captured comply with the Data Protection Act.

3.2 The academy will make every effort to position cameras so that their coverage is restricted to the academy premises, which may include outdoor areas.

3.3 Members of staff should have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring.

4. COVERT MONITORING

4.1 The academy may in exceptional circumstances set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

4.2 In these circumstances authorisation must be obtained from a member of the senior management team.

4.3 Covert monitoring must cease following completion of an investigation.

4.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

5. STORAGE & RETENTION OF CCTV IMAGES

5.1 Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

5.2 All retained data will be stored securely in a fire proof safe.

6. ACCESS TO CCTV IMAGES

6.1 Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.

7. SUBJECT ACCESS REQUESTS (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

7.2 All requests should be made in writing to the Principal. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.

7.3 The academy will respond to requests within 40 calendar days of receiving the written request and fee.

7.4 A fee of £10 will charged per request, all cheques are to be made payable to Derbyshire County Council.

7.5 The academy reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation.

8. ACCESS TO & DISCLOSURE OF IMAGES TO THIRD PARTIES

8.1 There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the academy where these would reasonably need access to the data (e.g. investigators).

8.2 Requests should be made in writing to the Principal.

8.3 The data may be used within the academy's discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

9. COMPLAINTS

9.1 Complaints and enquiries about the operation of CCTV within the academy should be directed to the Principal in the first instance.

FURTHER INFORMATION

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- www.ico.gov.uk
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 1998

Appendix A - Checklist

This CCTV system and the images produced by it are controlled by the Business Manager who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement of the Data Protection Act 1998).

	Checked (Date)	**By**	**Date of next review**
Registration with the Information Commissioner is done by the de Ferrers Trust			
There is a named individual who is responsible for the operation of the system.			
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Staff and members of the academy community will be consulted about the proposal to install CCTV equipment.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The 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.			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

APPENDIX B – CCTV SIGNAGE

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The academy is to ensure that this requirement is fulfilled.

THE CCTV SIGN SHOULD INCLUDE THE FOLLOWING:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the academy
- The contact telephone number or address for enquiries

APPENDIX C – DATA PROTECTION ACT

THE DATA PROTECTION ACT 1998: DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

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

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

This is not a full explanation of the principles, for further information refer to the Data Protection Act.