

The *Active Learning* Trust

CCTV POLICY

This policy is reviewed every three years

History of Document

Issue No	Author/Owner	Date Reviewed	Date Approved by Trust Board	Comments
1	DPO	June 2018	12 July 2018	1 st formal issue

1. INTRODUCTION

- 1.1 The Active Learning Trust (“Trust”) is fully committed to the safety of its staff, students and visitors and to this extent has invested in the security of its buildings and facilities.
- 1.2 This closed-circuit television (“CCTV”) Policy takes account of all applicable legislation and guidance, including:
 - 1.2.1 General Data Protection Regulation (“GDPR”) 2016
 - 1.2.2 Data Protection Act 2018
 - 1.2.3 CCTV Code of Practice produced by the Information Commissioner’s Office
 - 1.2.4 Human Rights Act 1998

2. PURPOSE OF THE POLICY

- 2.1 The purpose of this CCTV Policy (“Policy”) is to outline the Trust’s expectations on the management, operation and use of CCTV systems within the Trust.

3. RESPONSIBILITY

- 3.1 The Trust Board has ultimate responsibility for setting this Policy.
- 3.2 Headteachers are responsible for ensuring this Policy is implemented at their own school. Where the term Headteacher is used this incorporates Executive Headteacher roles where these exist and the Chief Executive Officer of the Active Learning Trust when the statement refers to the central Trust.
- 3.3 All staff should ensure that they comply with this Policy.
- 3.4 An Information Management & Cyber Security Governance Group reports to the Trust’s Senior Leadership Team and considers the use of CCTV within its data protection remit.
- 3.5 The Trust’s Data Protection Officer is responsible for providing guidance and advice on the use of CCTV and for monitoring schools’ compliance with this Policy.

4. USE OF CLOSED-CIRCUIT TELEVISION (“CCTV”)

- 4.1 The Trust uses CCTV for the following purposes:
 - 4.1.1 To provide a safe and secure environment for pupils, staff and visitors;
 - 4.1.2 To prevent the loss of or damage/vandalism to school buildings and/or assets;

- 4.1.3 To monitor the security of the schools' sites; and
- 4.1.4 To assist in the prevention of crime and assist the Police in apprehending offenders.

5. LOCATION OF CAMERAS

- 5.1 All CCTV cameras will be sited in such a way as to meet the purpose for which the CCTV is operated. Cameras will be sited in prominent positions where they are clearly visible to staff, pupils and visitors.
- 5.2 Cameras will not be sited, so far as possible, in such a way as to record areas that are not intended to be the subject of surveillance. Schools will make all reasonable efforts to ensure that areas outside of school premises are not recorded.
- 5.3 Cameras will not be sited in areas where individuals have a heightened expectation of privacy, such as changing rooms or toilets.

6. CCTV SIGNS

- 6.1 CCTV signs must be displayed at entrance points and where possible within the areas covered by the system to inform staff, students and the public that they are in an area within which CCTV is in operation.

7. DATA PROTECTION IMPACT ASSESSMENT (“DPIA”)

- 7.1 Prior to the installation of any CCTV camera, or system, a DPIA will be conducted by a school to ensure that the proposed installation is compliant with legislation and ICO guidance.
- 7.2 Schools will adopt a privacy by design approach when installing new cameras and systems, taking into account the purpose of each camera so as to avoid recording and storing excessive amounts of personal data.
- 7.3 Where CCTV cameras have historically been installed, prior to the issue of an ICO's CCTV Code of Practice, the Trust's Data Protection Officer will work with schools to undertake a retrospective Privacy Impact Assessment and/or DPIA.

8. LIVE VIEWING

- 8.1 The viewing of live CCTV images is restricted to members of staff approved by a Headteacher or designated person.
- 8.2 No other individual will have the right to view or access any CCTV images.

9. RECORDINGS

- 9.1 Schools will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images.
- 9.2 CCTV recording systems must be located in restricted access areas and only be viewed by approved staff authorised by a Headteacher when there is a clear reason for this to happen.
- 9.3 Recorded images will be stored in a way that ensures their integrity (e.g. password protected or encrypted) and in a way that allows specific times and dates to be identified.
- 9.4 The Trust reserves the right to use images captured on CCTV where there is activity that the Trust cannot be expected to ignore such as criminal activity, safeguarding, potential misconduct/gross misconduct, or behaviour which puts others at risk.
- 9.5 A log of downloaded CCTV images will be maintained by schools and kept in a secure manner. Such log will include the date that a recording was downloaded, reason, name of requestor, Headteacher authorisation to destroy and the date when it is destroyed.
- 9.6 Images retained for evidential purposes will be retained in a locked area accessible by a school's CCTV system administrator only.

10. DISCLOSURE OF IMAGES TO DATA SUBJECTS

- 10.1 Any individual recorded in a CCTV image is a data subject for the purposes of data protection legislation and has a right to request access to those images of themselves taken by a school's CCTV system.
- 10.2 When such a request is made, the process per the Trust's Subject Access Request Policy and associated written procedures and guidance is to be followed by a Headteacher and his/her nominated person who is authorised to process SARs. They will arrange for the CCTV footage to be reviewed by approved users, in respect of relevant time periods where appropriate, in accordance with the request.
- 10.3 If the footage contains only the individual making the request then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. A screen shot could be provided if the person is only shown in one footage.

10.4 If the footage contains images of other individuals then a school must consider whether:

10.4.1 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

10.4.2 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

10.4.3 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

11. DISCLOSURE OF RECORDED IMAGES TO THIRD PARTIES

11.1 A school must only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with data protection legislation.

11.2 CCTV images will only be disclosed to the Police in line with the purposes for which the CCTV system is in place.

11.3 If a request is received from the Police for disclosure of CCTV images then a Headteacher must follow the same process as per point 10.2 above in relation to subject access requests.

12. MAINTENANCE

12.1 CCTV systems are to be checked regularly to ensure that they are operating effectively.

13. RETENTION OF IMAGES

13.1 Recordings will be retained for a limited time period only and for no longer than their intended purpose. This will be up to a maximum of 30 days. All recordings are to be erased before disposal.

13.2 Downloaded recordings for subject access requests and third parties are to be generally retained for six months unless the Police requests that they be retained for a longer period of time.

14. STAFF TRAINING

14.1 A requirement under the ICO's CCTV code of practice is that personnel responsible for the system know how to manage the data and access the images. The effectiveness of the system depends on the quality of personnel selected for its operation. A Headteacher shall ensure that all appropriate staff are trained on the use of the equipment and familiar with their data protection responsibilities as detailed in the ICO's CCTV code of practice.

15. BREACH

- 15.1 In the unlikely event of photos or images of children being compromised through a data breach deemed to be a risk to the rights and freedoms of data subjects, a school must notify the Trust's Data Protection Officer who will notify the Information Commissioner's Office within 72 hours. Affected individuals will also be notified without undue delay.

16. MISUSE OF CCTV SYSTEM

- 16.1 The misuse of a school's CCTV system could constitute a criminal offence.
- 16.2 Any member of staff who breaches this policy may be subject to disciplinary action.

17. COMPLAINTS

- 17.1 Any complaints relating to this Policy or to the CCTV system operated by a school from a member of the public should be made in accordance with the Trust's Complaints Policy. Any complaints from a member of staff should be made in accordance with the Trust's Staff Grievance Procedure.

18. MONITORING AND REVIEW

- 18.1 This Policy will be monitored and reviewed every three years or in light of any changes to relevant legislation.