CCTV Policy

Date approved by Trustees of Ventrus Multi Academy Trust	**13th December 2023**
Review Period	**Annually**
Next Review Date	**December 2024**

Contents

1 INTRODUCTION

1.1 [insert school name] uses closed circuit television (CCTV) images to monitor the school's buildings in order to provide a safe and secure environment for pupils, staff and visitors, to reduce crime and to prevent loss or damage to school property.

1.2 The system comprises several fixed cameras.

1.3 The system capability records both sound and images.

1.4 The CCTV system is owned and operated by the school, the deployment of which is determined by the Headteacher, with support from the Trust Estates Manager.

1.5 The CCTV is monitored centrally from the school office by the Headteacher/Lead Administrator/Senior Site staff. (Delete as applicable)

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

1.7 The school's CCTV Scheme is registered with the Information Commissioner's Office under the terms of the Data Protection Act 2018. The use of CCTV, and the associated images and any sound recordings is covered by the General Data Protection Regulation 2016 (the GDPR) and the Data Protection Act 2018. This policy outlines the school's use of CCTV and how it complies with the data protection legislation.

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.

1.9 The school uses the Trust Data Protection Impact Assessment (DPIA) template when processing is considered a 'high risk activity': Systematic monitoring, Data concerning vulnerable data subjects and applying new technological or organisational solutions.

2 STATEMENT OF INTENT

2.1 The Trust 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: Codes of practice | ICO
All authorised operators will sign to agree they have understood this policy on an annual basis and/or when changes are made to this policy.

2.2 CCTV warning signs are clearly and prominently placed at all external entrances to the school, including school gates, where coverage includes outdoor areas. Signs contain details of the purpose for using CCTV. In areas where CCTV is used, the school ensures 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 of the camera placement is intended to ensure that the CCTV 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.

2.4 CCTV surveillance at the schools is intended for the purposes of:

- Protecting the school buildings and assets, both during and after school hours.
- Promoting the health and safety of staff, pupils, and visitors.
- Preventing bullying.
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- Supporting the police in a bid to deter and detect crime.
- Assisting in identifying, apprehending, and prosecuting offenders.
- Ensuring that the school rules are respected, so that the school can be properly managed.

3 SITING THE CAMERAS

3.1 Cameras are 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 school will ensure that the location of equipment is carefully considered in consultation with the Estates Manager to ensure that images captured comply with the GDPR and the Data Protection Act 2018.

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

3.3 CCTV will not generally be used in classrooms, but in areas within the school that have been identified as not being easily monitored. If CCTV is placed in classrooms, there must be advanced written consent of the Executive Leadership Team and parents must be consulted in advance; a DPIA would be completed by the Headteacher and agreed by a Director of School Improvement, in consultation with the DPO.

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

4 COVERT MONITORING

4.1 The school may in exceptional circumstances set up covert monitoring, for example:

- 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.
- 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, with advanced written consent, by the Headteacher from the Executive Leadership Team and the Data Protection Officer.

4.3 A data protection impact assessment will be carried out, by the Headteacher, prior to any covert monitoring and must be signed off by the Data Protection Officer and Director of School Improvement.

4.4 Covert monitoring must cease following completion of an investigation.

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

5 STORAGE AND RETENTION OF CCTV IMAGES

5.1 Recorded data is retained in accordance with the retention of records schedule. 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 Only the Headteacher, or a member of the Executive Leadership Team, will be permitted to download, store and/or retain CCTV images and/or sound files. Downloads should only be stored in Office 365, and password protected.

5.3 All retained data will be stored securely, by the Headteacher, or member of the Executive Leadership Team, in the Ventrus One Drive.

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 unless responding to a formal SAR, and under the guidance of the DPO, which should be sought in advance.

7 SUBJECT ACCESS REQUESTS (SAR)

7.1 Individuals have the right to request access to CCTV footage relating to themselves under the GDPR and the Data Protection Act 2018.

7.2 All requests should be made to the school, verbally or via email to DPO@ventrus.org.uk 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 Headteacher must contact the DPO immediately for advice.

7.4 The school will respond to requests within 1 month of receipt. Schools are advised to investigate and respond promptly to avoid the footage being overwritten.

7.5 Under data protection legislation, a fee is not normally charged, although a reasonable fee based on the administrative cost of providing the data can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive.

7.6 The school reserves the right to refuse access to CCTV images and sound footage where this would prejudice the legal rights of other individuals, jeopardise an on-going investigation or where the images/sound relate to, or identify persons, other than the subject of the request.

8 ACCESS TO AND 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 school, where these would reasonably need access to the data (e.g. investigators). These will be actioned once a completed Ventrus School Data Request form (SAR) has been submitted and guidance from the DPO has been sought.

8.2 Any parent requests should be made to the school, verbally or via email to DPO@ventrus.org.uk marked for the Headteacher's attention and treated as a Subject Access Request. Parents can view the footage, but only if no other pupil(s)' images are on view. Redacted screen prints should be considered as an alternative.

8.3 Any access by staff should comply with the following: live footage should only be seen by staff managing or monitoring the system/cameras, with the delegated authority of the Headteacher. Recording systems must be in areas of reduced access, to avoid potential tampering.

8.4 The data may be used within the Trust'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 school should be directed to the Headteacher in the first instance, who will consult with the Data Protection Officer, and act in accordance with the Trust Complaints Policy and Procedures.

10 FURTHER INFORMATION

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

- CCTV Code of Practice Revised Edition V1.2 2017 (published by the Information Commissioners Office) www.ico.org.uk
- Biometrics and Surveillance Cameras Commissioner Feb 2022 https://www.gov.uk/government/organisations/surveillance-camera-commissioner
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 2018
- General Data Protection Regulation 2016 (GDPR)

Appendix 1 Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
V.1 10.1	Updated ICO & Commissioners link	SLD	26/10/2021
V.2 2.1	Updated Codes of Practice	SLD	25/10/2022
V.2 5.3	Amended Ventrus equipment from One Drive storage	SLD	25/10/2022
V.2 10.1	Biometrics and surveillance name change	SLD	25/10/2022
V.3	Additional security updates	SLD	30/05/2023
V.4 1.9	Rewording of retention of data & adding reference to the Trust DPIA	SLD	25/10/2023