



SPARKEN HILL
ACADEMY

UK GDPR CCTV Policy

Rev	Date Issued	Prepared By	Approved	Review Date	Comments
1.2	Feb 2021	RTL	Feb 2022	Feb 2023	

Introduction

- 1 Introduction
- 2 Objectives of the CCTV system
- 3 Statement of intent
- 4 Operation of the system
- 5 Storing and Viewing of CCTV Images
- 6 Requests to view or have copies of images by external agencies or individuals
- 7 Breaches of the code (including breaches of security)
- 8 Assessment of the scheme and code of practice
- 9 Complaints

1 Introduction

- 1.1 The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system for Sparken Hill Academy. The Policy follows the Information Commissioner's CCTV Code of Practice.

2 Objectives of the CCTV system

- 2.1 To ensure the personal safety of students, staff and visitors;
- 2.2 To reduce the fear of crime;
- 2.3 To protect the school buildings and their assets;
- 2.4 To support the police in a bid to deter and detect crime;
- 2.5 To assist in identifying, apprehending and potentially prosecuting offenders;
- 2.6 To protect members of the public and private property; and
- 2.7 To assist in managing the school.

3 Statement of intent

- 3.1 The CCTV is part of our registration with the Information Commissioner's Office (ICO) under the terms of the Data Protection Act 2018.
- 3.2 The school will treat the system and all information, documents and recordings obtained and used as personal data under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018.
- 3.3 Cameras are used to monitor activities within the school and the grounds to identify adverse activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and wellbeing of the school's students, staff and visitors.
- 3.4 Images from private homes and gardens are kept out of range of the cameras and cannot be seen by the operator.
- 3.5 Materials or knowledge secured as a result of CCTV use will not be used for any commercial or media purpose. Information transferred to CD/DVD (or other appropriate media) will only be used for the investigation of a specific crime or incident.
- 3.6 The system has been designed to ensure maximum effectiveness and efficiency but it is not possible to guarantee that the system will cover or record every single incident taking place in the areas of coverage.

- 3.7 Warning signs, as required by the Code of Practice of the Information Commissioner, have been displayed.

4 Operation of the system

- 4.1 The overall management of the CCTV system will be overseen by the member of the Senior Leadership Team with responsibility for the school premises. They are responsible for ensuring that the CCTV system is operated according to this policy and that regular audits are carried out to ensure that procedures are complied with. They are also responsible for the annual registration with the Information Commissioner. The DPO is responsible for this policy and for conducting the regular, and at least annual, audits of the CCTV system.
- 4.2 The day-to-day management, administration, maintenance, security and support of the system will be the responsibility of the Principal.
- 4.3 The CCTV system will operate 24 hours each day, every day of the year, recording all activity in the areas covered. We ensure that our monitors are correctly sited, taking into account the images that are displayed.
- 4.4 Recordings will be held on system memory for a period of 28 days and then deleted. The DPO is responsible for deciding what images will be retained, if required. The Principal is responsible for maintaining the recordings, ensuring their security and deleting them within the specified time period.

5 Storing and Viewing of CCTV Images

- 5.1 Recorded material is stored in a way that maintains the integrity of the information and keeps it secure. This is to ensure that the rights of individuals recorded by the CCTV are protected and that the information can be used as either evidence in court or for the management of the school, as and when required.
- 5.2 If we are keeping information that may be used as evidence in court or for management of the school, we will keep a record/audit trail of how the information is handled.
- 5.3 Recorded images will be viewed by the nominated person/s for the site. The images will be viewed in a secure and nominated location. The monitoring or viewing of images is restricted to the DPO, the Principal or persons designated by the Principal, subject to any Subject Access Requests or requests by law enforcement.
- 5.4 Where images are in an area of particular sensitivity such as a changing room, we will only view recorded images after an incident has occurred.

- 5.5 The only person authorised to make copies (electronic or paper) of images is a member of SLT, or another person specifically directed by the Principal or the DPO.
- 5.6 All data stored for investigated purposes will be stored in accordance with our data retention policy. Upon completion of any internal or external investigation the data will be transferred from the network to an external storage device such as a CD or an encrypted USB stick.

6 Requests to view or have copies of images by external agencies or individuals

- 6.1 The DPO will review all requests for disclosure of CCTV images. Such requests can be made under the GDPR, the Data Protection Act 2018 or the Freedom of Information Act 2001. Such requests may come from the police, solicitors or individuals. All requests will be considered in line with our Subject Access Request Policy.
- 6.2 When disclosing surveillance images of individuals, the DPO will consider if obscuring of identifying features is necessary or not. This will depend on the nature and context of the footage that is being considered for disclosure.

7 Breaches of the code (including breaches of security)

- 7.1 The Principal, or a senior leader acting on their behalf, will initially investigate any breach of the Code of Practice by school staff. Any serious breach of the Code of Practice will be subject to the terms of disciplinary procedures already in place.
- 7.2 A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed will be investigated by the DPO.

8 Assessment of the scheme and code of practice

- 8.1 The Principal, the DPO, or their representative, may carry out performance monitoring, including random operating checks.

9 Complaints

- 9.1 Any complaints about the schools' CCTV system should be addressed, in the first instance, to the DPO, who will investigate all complaints in accordance with the Information Commissioner's Code of practice.