



WELLESLEY PRIMARY SCHOOL

CCTV Policy

Issue No: 6
Date: January 2025

Approved by Governors: 30th January 2025

Contents

Change Record Sheet.....	1
Summary.....	1
Introduction	2
Objectives of the CCTV Policy	2
Statement of intent	2
Operation of the system.....	3
Control and Liaison	3
Monitoring procedures.....	3
Breaches of the code (including breaches of security).....	4
Complaints	4
Access by the Data Subject	4
Public information	4

Change Record Sheet

Issue No	Date	Summary of Change	Amended by:
3	March 2016	Policy Reviewed	Heather Small
4	May 2018	Policy Updated – GDPR	Kathryn Jones
5	March 2019	Policy Review	Heather Small
6	January 2025	Policy Updated – use of CD/DVD removed and replaced with USB drives	Kathryn Jones

Summary

This policy will be reviewed every 3 years.

This policy has been reviewed to ensure that it meets the requirements of the equalities impact assessment.

Policy Written: November 2011

Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at Wellesley Primary School. The system comprises of two mini-dome cameras located on the school building. All cameras are controlled from the Office and the system can only be accessed by nominated Senior Leaders and Administrative staff. The school owns the CCTV system.

The Policy will be subject to review by the Governors. This Policy follows the General Data Protection Regulation guidelines.

Objectives of the CCTV Policy

The objectives of the School's use of CCTV are:

- a) To increase personal safety of students, staff and visitors, and reduce the fear of crime
- b) To protect the school buildings and their assets
- c) To support the Police in a bid to deter and detect crime
- d) To assist in identifying, apprehending and potentially prosecuting offenders
- e) To protect members of the public and private property

Statement of intent

The CCTV Scheme has been registered with the Information Commissioner under the terms of the Data Protection Regulation 2018 and will seek to comply with the requirements both of the General Data Protection Regulation and the Commissioner's Code of Practice. The school will treat the system and all information, documents and recordings obtained and used as data protected by the Regulation.

Cameras will be used to monitor activities within the school grounds in the vicinity of the access gates to identify adverse activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and wellbeing of pupils and staff, together with its visitors. Static cameras are positioned to ensure they do not focus on private homes, gardens and other areas of private property. At no time will a camera be directed to follow or track an individual as all the currently deployed cameras are fixed.

Materials or knowledge secured as a result of CCTV use will not be used for any commercial purpose. USB drives will only be released for use in the investigation of a specific crime and with the written authority of the police. Footage will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the CCTV Scheme will give maximum effectiveness and efficiency within available means, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the school's CCTV system.

Operation of the system

The CCTV system will be administered and managed by the school in accordance with the values and objectives expressed in the code. The day to day management will be the delegated responsibility of the Head/School Business Manager during the day, and the Caretaker out of hours and at weekends.

The CCTV system will operate 24 hours each day, every day of the year, recording all activity.

Control and Liaison

The system provider will periodically check and confirm the efficiency of the system and, in particular, that the equipment is properly recording and that cameras are functional. The school will liaise with Avon Alarms regarding servicing and/or repairs and maintenance of the system.

Monitoring procedures

Camera surveillance may be maintained at all times and footage continuously recorded and held on system memory for approximately 2.5 weeks

To maintain and preserve the integrity of any USB drive used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention will be strictly adhered to:

- (a) Each USB drive must be identified by a unique reference number.
- (b) Before using, each USB drive must be cleared of any previous recording.
- (c) The person responsible for recording will register the date and time of the recording, including the USB drive reference number.
- (d) A USB drive required for evidential purposes must be sealed, witnessed, signed by the member of staff responsible for the recording, dated and stored in the safe. If a USB drive is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the member of staff, dated and returned to the safe.

USB drives may be viewed by the Police for the prevention and detection of crime. A record will be maintained of the release of the USB drive to the Police or other authorised applicants. A register will be maintained for this purpose.

Viewing of footage by the Police or any external individual must be recorded in writing and entered in the register. Requests by the Police can only be authorised under section 29 of the General Data Protection Regulations 2018. Should a USB drive be required as evidence, a copy may be released to the Police under the procedures described in paragraph 6(d) of this Code.

CCTV

USB Drives will only be released to the Police on the clear understanding that the USB drive remains the property of the school, and both the USB drive and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the Police to pass to any other person the USB drive or any part of the information contained thereon.

On occasions when a Court requires the release of an original USB drive this will be produced from the safe, complete in its sealed bag.

The Police may require the school to retain any stored USB Drives for possible use as evidence in the future. Such drives will be properly indexed and securely stored until the Police need them.

Applications received from outside bodies (e.g. solicitors) to view or release footage stored on DVD/CD's will be referred to the Headteacher. In these circumstances USB drives will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, or in response to a Court Order. A fee may be charged in such circumstances.

Breaches of the code (including breaches of security)

The Headteacher, or a senior leader acting on her 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.

Complaints

Any complaints about the schools' CCTV system should be addressed to the Headteacher. Complaints will be dealt with in accordance with the ICO Code of Practice.

Access by the Data Subject

The General Data Protection Regulations provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about them, including those obtained by CCTV. Requests for Data Subject Access should be made through the Headteacher.

Public information

Copies of this policy will be available to the public from the school website or from the School Office.