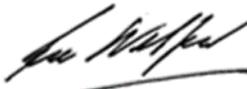




CCTV Policy

Policy Date:	June 2021	Version: 1.1		
Policy Review Date:	June 2023	Headteacher Debra Bailey		28/06/2021
Ratified by Governing Body:				
Sue Welford (Chair of Governors)				28/06/2021

Document Control Ref:	BLS/WW/001
Document Location:	Electronic document on T drive (shared with all staff) Hard copy with Business Manager
Document Owner:	School Business Manager
Review Period:	Every 2 years or unless significant changes to legislation

Revision History

Version	Date	Reviewed By	Amendment Details
1.0	June 2021	BLS review	Some wording simplified

CONTENTS

1. Introduction	2
2. Scope	3
3. Requests for access to the system.....	6

1. Introduction

Rushey Mead Primary School (RMPS) operates a Closed-Circuit Television (CCTV) surveillance system ("the system") on the premises, with images being monitored and recorded centrally. The system is owned, operated and managed by RMPS. Images obtained from the system, which include recognisable individuals, constitute personal data and are covered by the UK GDPR and Data Protection Act 2018. This policy should, therefore, be read in conjunction with RMPS's other data protection policies.

To comply with the UK GDPR and Data Protection Act 2018, RMPS, as an organisation and Data Controller which collects and processes personal data, must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to, personal data from its collection or creation, through to how it is stored, all actions performed with and on the data, through to, and including, its disposal.

This means in relation to any information held about individuals, RMPS will hold only information which is necessary for our legitimate business interests and will restrict access generally to a "need to know basis" and ensure that its managers only hold 'current' necessary information.

This policy has been drawn up in accordance with the guidance contained within the Information Commissioner's CCTV Code of Practice and the Home Office Surveillance Camera Code of Practice.

The primary purpose and lawful basis within our legitimate interests for use of CCTV by RMPS is defined as:

"RMPS CCTV is used for maintaining public safety (including the safeguarding of children), the security of property and premises and for the detection, prevention and investigating of crime. It may also be used

to monitor staff when carrying out work duties. For these reasons, the information processed may include visual images, including personal appearance and behaviour of those displayed and recorded on the system”.

This policy sets out the RMPS arrangements to ensure the management, operation and use of CCTV is regulated to provide consistency and compliance with relevant legislation.

2. Scope

The RMPS CCTV system may record pupils, employees, contractors, visitors, offenders and suspected offenders, members of the public and those on our premises, entering or in the immediate vicinity of the main area under surveillance. RMPS recognises the potential intrusive effect of such systems on individuals and their right to privacy.

This policy also takes into account the:

- Requirements for processing personal data as set out in the UK GDPR and Data Protection Act 2018
- Protection of Freedoms Act 2012
- Right to privacy as set out in Article 8 of the Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Crime and Disorder Act 1998 (regarding disclosure to investigators)

This policy applies to all RMPS employees and those handling CCTV data on behalf of RMPS including, but not limited to:

- Third parties involved in the design, development, provision or operation of CCTV information systems or services for RMPS;
- Access to RMPS information from remote locations where the CCTV, and computer and network facilities are not under the control of RMPS;
- Users who are not employees of RMPS and require access to RMPS CCTV information or CCTV systems;
- All employees, including contractors, temporary staff and third parties employed directly and indirectly by the 3rd Party organisation (e.g. subcontractors).

Images captured by the system are recorded continuously and may occasionally be monitored real time/live by RMPS. No images displayed on monitors are visible from outside RMPS premises. The images are kept securely on the school servers, and access to operate the system is strictly limited to trained and authorised individuals who need to access the system for necessary and proportionate reasons.

No images, recordings or information gathered by the system shall be stored any longer than is required for the stated purpose. Relevant images or recordings or information will be deleted once their purpose has been discharged.

If there is no legitimate reason to keep the recording, the data will be erased - in normal use, images are overwritten and deleted automatically every 30 days.

Where any new CCTV system is proposed the Data Protection Officer should be consulted and a data protection impact assessment will be completed to demonstrate that the new system is necessary and complies with data protection legislation.

All staff with access to RMPS CCTV system are trained and made aware of the sensitivity of handling CCTV images and recordings. The DPO will ensure that authorised staff are fully briefed and trained in all aspects of the operational and administrative functions of the system.

Specialist training in CCTV compliance is available to support those expected to use, monitor and disclose CCTV images. Managers must also make their employees aware that the disclosure, or improper use, of personal data may result in criminal prosecution and/or disciplinary action.

All access to recorded images must be approved and recorded by the School Business Manager. Access to images is restricted to those who need to have access in accordance with this standard and any governing legislation, or to support the police in their role to prevent and detect crime.

Disclosure of recorded material will only be made to third parties in accordance with the purposes of the system and in compliance with the UK GDPR and Data Protection Act 2018.

3. Requests for access to the system

All requests for access to the system should be made to the Business Manager at the school.

CCTV images are covered under the school Subject Access Request Policy which outlines the process for how the school complies with requests for personal data and should be consulted in the first instance.

Requests from the police for access to images should be referred to the Headteacher or School Business Manager.

This policy should be read in conjunction with the Data Protection Policy, the Subject Access Request Policy* and the Data Breach Policy*.

*** The Subject Access Request Policy and the Data Breach Policy will be available from September 2021.**