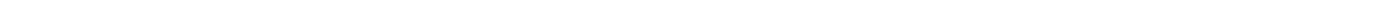


THIS POLICY APPLIES TO THE TRUST BOARD, THE CENTRAL SERVICES TEAM
AND ALL TRUST SCHOOLS/ACADEMIES

	September 2024
	September 2025
	3.0
	Chief Operating Officer

Hope Sentamu Learni



Protection of Freedoms Act 2012
School Standards and Framework Act 1998
Children Act 1989 and 2004
Equality Act 2010
Surveillance Camera Code of Practice 2013
Regulation of Investigatory Powers Act 2000
The Education (Pupil Information)(England) Regulations 2005 (as amended in 2016)

3.2. This policy has been created with regard to the following statutory and non-statutory guidance:

DfE (2022) 'Protection of biometric data of children in schools and colleges'
'The Surveillance Camera Code of Practice' - Home Office (2021)
'Guide to the UK General Data Protection Regulation (UK GDPR) ICO 2021'
'In the picture: A data protection code of practice for surveillance cameras and personal information' ICO (2017)
ICO (2022) 'Video Surveillance'

3.3. This policy operates in conjunction with the following Trust policies:

Photography and Videos in Schools Policy
E-Safety and Acceptable Use Policy - Pupils
E-Safety and Acceptable Use Policy - Staff and Authorised Users
Freedom of Information Policy
Data Protection (UK GDPR) Policy

4.1.

The Trust Board is ultimately responsible for the systems and ensuring compliance with each school/academy.

4.2.

The role of the Data Protection Officer (DPO) includes:

Dealing with Freedom of Information requests and Subject Access Requests (SARs) in line with legislation, including the Freedom of Information Act 2000.

00

ne
Enclud ng
line

w

Inforin

Ensuring that the processing of biometric data is done so in line with the Trust's Protection of Biometric Data Policy.

5.1. To protect the school/academy building and their assets. The systems function is to:

Maintain a safe environment

Ensure the welfare of pupils, staff and visitors

Detect criminal acts against persons and property

Assist the Police in identifying persons who have committed an offence

- 10.5. The Police may require the school/academy to retain the stored media for possible use as evidence in the future. Such media will be correctly indexed and securely stored until they are needed by the Police.
- 10.6. Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Headteacher/Principal.

B60

- 11.1. Any breach of the Code of Practice by school/academy staff will be investigated by
-

14.6. The

15.2. Individuals have the right to have their personal data erased if:

The data is no longer necessary for the original purpose it was collected for.

The data processor relies on legitimate interests as a basis for processing, the data subject objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.

The data has been processed unlawfully.

There is a specific legal obligation.

15.3. There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

Where the processing is needed for the performance of a task in the public interest or an official authority.

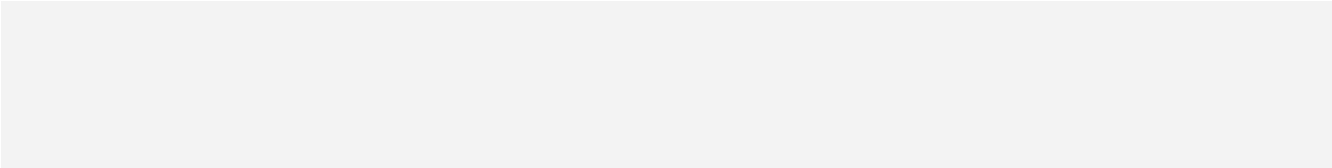
Certain research activities.

Compliance with a specific legal requirement.

15.4. All media captured by CCTV imaging belongs to, and remains the property of the school/academy.

15.5. The school/academy will verify the identity of any person(s) making a Subject Access Request (SAR) before any information is supplied. Please refer to the Trust's Subject Access Request Policy and Procedures for further details.

15.6. Requests by persons outside the school/academy for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher/Principal, who will consult the DPO, on a case-by-case basis.

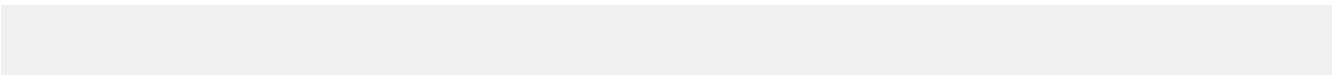
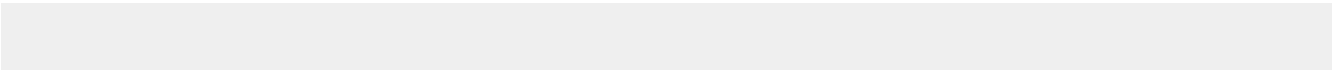
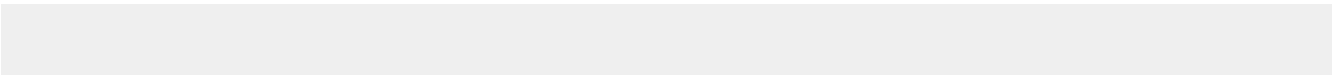


Manor Church of England Academy

Jordan Cairns

September 2024

In conjunction with the Trust wide CCTV Policy, localised procedures have been established to ensure that
w



Please see the below details of the person(s) responsible for investigating breaches of the code of practice and/or security breaches.

e

