Information Governance Policy

Chisenhale Primary School

Confidence • Curiosity • Kindness

Date reviewed	November 2025
Written by	Connetix IG – Sue White
Approved by Governors	Resources February 2026
Planned Review date	Resources February 2028

Data Protection, FoI Policy and CCTV

Data Protection Policy

1 PURPOSE OF THIS POLICY

The objective of this policy is to ensure that:

- all data processing carried out by the school complies with data protection legislation and is in line with the data protection principles
- all members of staff are aware their obligations under the General Data Protection Regulation (GDPR) and associated data protection laws

This policy also signposts the procedures in place to support implementing this policy.

2 LEGISLATION

The school is subject to the following laws in regard to this data:

- The **UK General Data Protection Regulation (UK GDPR)** - sets out the data protection principles and legal basis for processing, the rights of data subjects, the obligations of data controllers and processors, international transfers, and enforcement
- The **Data Protection Act 2018 (DPA 2018)** - sets out the data protection framework for UK data protection law, defining exemptions and the powers of Information Commissioner's Office (ICO), the UK's regulator for data protection and freedom of information law
- The **Privacy and Electronic Communications (PECR)** - These regulations provide a range of rules around electronic communications. The school will most commonly follow these for the use of cookies on its websites and emails

The school is registered with the Information Commissioner's Office as a 'data controller', registration number Z6810737. The school is defined as a ‘public authority’ in Schedule 1 of the Freedom of Information Act 2000 and therefore is defined as a public authority in the UK GDPR and DPA 2018. Breaching the UK's privacy laws can result in enforcement action, including monetary penalties.

3 DEFINITIONS

The following terminology is used in the legislation:

Personal Data

Data which relates to an identifiable living individual, which is being processed automatically or recorded as part of a relevant, filing system.

Special Category Data

Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data,

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Criminal Convictions Data

Personal data relating to criminal convictions and offences or related security measures.

Data Controller

A person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data Subject

An individual who is the subject of personal data.

Data Processor

A person or organisation who processes data on behalf of the Data Controller and according to their instructions.

Processing

Obtaining, accessing, altering, adding to, deleting, changing, disclosing or merging data and any other action that can be carried out with data.

4 SCOPE

This policy applies to:

- all employees at the school
- all contractors and suppliers in the services they carry out for the school

5 RESPONSIBILITIES

The Data Protection Officer ("DPO")

- informs and advises the school and its employees about their obligations to comply with the GDPR and other data protection laws
- reports to the Headmaster and Governors on data protection compliance
- monitors compliance with the GDPR and other data protection laws
- manages internal data protection activities
- advises on data protection impact assessments (DPIAs)
- trains staff and conducts internal audits
- they are the first point of contact for supervisory authorities and for data subjects

The school's Data Protection Officer is Naomi Korn Associates Ltd, contactable at IG@connetix.co.uk

Headmaster and Governors

- ensure that the school has appropriate resources and authority to carry out their function
- ensure that staff within their own area are fully aware of their obligations under the data protection laws and this policy to ensure compliance

All staff

- responsible for processing personal data securely and in line with this policy and associated procedures.
- ensure they have undertaken their mandatory data protection training
- aware that misuse of data by a member of staff can result in disciplinary action and a possible criminal record

The school's third-party suppliers or contractors

- processing personal data on our behalf in a secure and lawful manner
- follow our contractual instructions in regard to the processing of personal data
- ensure they and their staff are appropriately trained in data protection law and associated procedures

6 DATA PROTECTION PRINCIPLES

The seven data protection principles are set out in the UK GDPR:

Lawfulness, fairness, and transparency - The school explains to its pupils, staff, and other data subjects how it processes their personal data at the point of collection, what the legal basis is for processing and for what purposes the data will be used. In circumstances where the data is not sourced from the individual, information is made available which explains how the data is used.

Purpose limitation - The school only uses the personal data it has for the purposes it was collected for unless certain safeguards around re-use apply.

Data Minimisation - The school only collects personal data which is relevant to the purposes for which it is collected.

Accuracy - The school ensures that personal data is correct, up to date and it is able to be rectify any mistakes quickly.

Storage Limitation - The school does not retain personal data for longer than it is needed unless certain safeguards around long term or permanent storage apply.

Integrity and Confidentiality - The school protects their personal data against unauthorised access, loss, or destruction by a range of security measures.

Accountability - The school will be responsible for its data processing and be able to demonstrate compliance with the other data protection principles.

7 LEGAL BASIS FOR PROCESSING DATA

The school is required to have a legal basis in place for processing personal data.

The available legal bases are as follows, with some illustrative examples:

Legal basis	Example for the school
Data subject has given their consent	A parent has given consent on behalf of their child to appear in a promotional photo on the school's publication
Data subject is party to a contract with the school	A member of staff is employed by the school and their details are stored in their personnel file
The school has a legal obligation to process the data	The school is required to provide data to the central government
The data subject's vital interests are at stake, and they cannot give consent	A pupil has a medical emergency at the school and relevant details are provided to emergency services
The data processing is part of the school's function as an education provider	The school records the marks and assessment data for its pupils
The data processing meets a legitimate interest for the school or another party	The school uses its data to create aggregated statistics to monitor outcomes and plan new projects

The processing of Special Category Data requires an additional legal basis under GDPR and, in some cases, a substantial public interest condition from the Data Protection Act 2018. The processing of Criminal Convictions data requires a substantial public interest condition from the Data Protection Act 2018. In most cases the processing of this type of data will be related to a legal obligation around health and safety, equality or employment law.

The legal bases for each type of processing the school carries out will be recorded in the school's Record of Processing Activities (ROPA – please see the 'Record keeping' section below) and communicated to data subjects in the school's Privacy Notice (see the 'Privacy and transparency' section below).

8 RIGHTS

The school will ensure that staff, pupils and other data subjects are aware of their rights in regard to their data and have in place processes to deal with rights requests in a timely and compliant manner. Requests are in most cases free, and the school has 30 days to respond. In exceptional cases 30 days can be expanded to 90 and a fee can be charged. These rights are not absolute, and the school will explain in its response the reasons behind any refusal or withholding of information. To make a GDPR rights request please contact IG@connetix.co.uk

9 PERSONAL DATA BREACHES

The school will ensure it has an agreed procedure for identifying and managing personal data breaches, in line with UK GDPR Article 33 (notification of a breaches to the Information Commissioner's Office) and 34 (notification of breach to data subjects).

10 DATA PROTECTION BY DESIGN

The school will ensure that it ensures all new projects are implemented with the data protection principles embedded from the start. All new projects involving the processing of personal data with a high risk to individuals will require a Data Protection Impact Assessment (DPIA) to be carried out.

11 RECORD KEEPING

The school will ensure it documents its processing activities in accordance with GDPR Article 30, listing the data it collects, the categories of data subjects and the legal basis for processing. The Record of Processing Activities (ROPA) will be maintained by the school's Data Protection Officer.

12 DATA PROCESSORS

The school will appoint data processors to process personal data on its behalf and according to its instructions. All data processors will be appointed under the terms of a written contract including commitments to process personal data in line with the responsibilities of processors set out in GDPR Article 28. Data processors will be listed in the Record of Processing Activities (ROPA).

13 INFORMATION SHARING

Where the school is required to routinely share personal data with another agency in government (local or central), education or health, it will ensure that a suitable information sharing agreement is in place to determine the fair and lawful sharing of personal data.

Ad hoc sharing with the police or other third parties will be carried out within the legal framework of the exemptions in the Data Protection Act 2018. Any instances of this type of sharing will need the required documentation from the requestor and be logged with the Data Protection Officer.

14 SECURITY

The school will ensure the integrity and confidentiality of its personal data by ensuring appropriate technical measures, in both physical and digital format, are in place. This will include cyber security, polices and procedures and staff training.

15 PRIVACY AND TRANSPARENCY

The school will ensure a comprehensive privacy notice is available to all data subjects, describing the purposes for processing, the school's legal basis to do and all information required by GDPR articles 12 to 14.

16 INTERNATIONAL DATA TRANSFERS

If the school or one of its data processors transfer data outside the UK or EEA, then one of the following arrangements will be in place:

- The transfer will be to a country with an "adequacy finding" by the UK or EU
- The transfer will be covered by an appropriate safeguard, such as the International Data Transfer Agreement (ITDA) or the Standard Contractual Clauses (SCC)
- In exceptional circumstances, the transfer may be covered by a derogation in the UK GDPR or an exemption in the Data Protection Act 2018

17 FREEDOM OF INFORMATION ACT 2000 (FOIA)

The school is a public authority and will receive Freedom of Information Act (FOIA) requests. The school will not disclose personal data in FOIA requests if to do so would breach the data protection principles. In some cases, it may not breach the principles (an example would be senior management team professional email addresses) and the school will disclose personal data to comply with the obligations of FOIA.

18 CONFIDENTIALITY OF PUPIL CONCERNS

If a pupil raises concerns with a member of staff, the school will maintain confidentiality unless it has safeguarding obligations to disclose the information to relevant third parties.

Freedom of Information policy

1 THE SCHOOL'S OBLIGATIONS

The public have a right to ask for information held by Chisenhale Primary School under the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR).

Chisenhale Primary School, has 20 school days, or 60 working days, whichever is shorter, in which to respond to FOIA or EIR requests. Both the FOI and EIR have "exemptions" or "exceptions" – circumstances under which we can legitimately refuse to provide some or all of the information requested. The school will always explain its reasons for refusing, and requesters have a right to ask us to review our decision.

The school is also required by FOIA to maintain a publication scheme where it proactively publishes certain types of information in a framework set by the Information Commissioner's Office. The document is on the school website https://chisenhale.towerhamlets.sch.uk

2 HOW WE MANAGE REQUESTS

FOIA requests should be submitted to info@chisenhale.towerhamlets.sch.uk

If staff directly receive a request quoting Freedom of Information or the Environmental Information Regulations, they will forward it to the Headteacher as soon as they can.

2.1 Clarifying requests

If it is not clear what the requester is asking for, the school can ask them to clarify their request. The 20 working day 'clock' then stops until clarification is received.

2.2 Withholding information

There are a number of exemptions in FOIA ('exceptions' in EIR) where the school can withhold information. The most common are:

- Where the information is already available to the public
- Where the information is due to be formally published at a future date
- Where disclosing the information would prejudice the prevention or detection of crime
- Where disclosing the information would affect the running of the school and undermine its internal planning and discussion
- Where disclosure would affect the health and safety of individuals
- Where disclosure would breach the data protection principles
- Where disclosure would breach the school's duty of confidentiality
- Where information requested is subject to legal professional privilege
- Where disclosure would prejudice the school's commercial interests or those of their contractors

There are other grounds for refusal under FOIA, where:

- It will take more than 18 hours to determine we hold the information, locate, extract and retrieve it
- The request is vexatious, according to range of criteria defined in law

If the school has concerns about disclosing the information requested, they will raise this with DPO at IG@connetix.co.uk as soon as possible, so any relevant exemption can be applied correctly.

2.3 Reviews and appeals

If a requester is unsatisfied with the response to their request, they can request an internal review. An internal review is carried out by a senior member of staff and allows the school to revisit how the request was handled and whether exemptions were applied correctly. An internal review should take no longer than 20 school days, though in exceptional cases may take longer.

2.4 The Information Commissioner

If the requester is unsatisfied with the outcome of the internal review, they may escalate the request to the Information Commissioner's Office (ICO). The ICO will investigate the request and decide on whether the school has correctly complied with FOIA in the handling of the request. They may,for example, require the school to disclose information it claimed was exempt.

CCTV Policy

Chisenhale Primary School operates and maintains a CCTV system to ensure the safety of its staff, pupils and visitors and to assist in the prevention / detection of crime and the prosecution / apprehension of offenders

Chisenhale Primary School is the data controller for the footage and images manages this information in accordance with UK General Data Protection Regulation (GDPR), the Data Protection Act 2018 and associated legislation.

1. PURPOSES OF THE CCTV SYSTEM

1.1 Purposes of the CCTV system

Chisenhale Primary School operates and maintains a CCTV system for the following purposes:

a) to ensure the safety of its staff, pupils and visitors
b) to assist in the prevention / detection of crime
c) to assist the prosecution / apprehension of offenders

1.2 Not in scope for the CCTV system

Chisenhale Primary School will not use the CCTV system for the following:

a) to collect audio recordings
b) for the collection and use of biometric data (such as face recognition technology)
c) to monitor staff in the normal duties of their work
d) to carry out covert surveillance (recording without clear signage)

1.3 Legal basis for processing personal data

The school's legal basis for processing personal data in footage and images is Article 6 (1) (e) of the UK GDPR, which allows us to process personal data when this is necessary to perform our public tasks as a school.

2. MAINTENANCE AND OPERATION

2.1 Data Protection Impact Assessment (DPIA)

Chisenhale Primary School has carry out a Data Protection Impact Assessment (DPIA) of the implementation of its CCTV system. Any changes to the use or purposes of the CCTV system set out in this policy will require a review and update of the Data Protection Impact Assessment (DPIA) to be carried out before installation.

2.2 Signage

The school provides clear signage explaining that CCTV is in operation, for what purpose and by whom and how to access further information.

2.3 Access to the CCTV system

Access to the CCTV system and footage will be documented in a procedural manual. Access will be restricted to named staff and protected by appropriate physical and technical measures.

2.4 Training

Staff accessing the CCTV system will be appropriately trained in the use of the system and the data protection issues around the footage and images.

2.5 Retention

The school retains the CCTV footage and images for a period of 30 days unless specific footage is required for an investigation in line with the purposes of this policy. All data will be securely destroyed, and the destruction recorded for audit purposes.

2.6 Maintenance

The CCTV system will be regularly checked, and any faults or issues reported and corrected as soon as possible.

2.7 Monitoring

The school's premises manager and head teacher will report as required on the management of the system, maintaining the following records:

a) A location map / inventory of all cameras
b) Records of deletion
c) Records of data sharing
d) Records of any footage or images being retained outside of the standard retention policy
e) Records of faults and the progress of their resolution
f) Data Protection Impact Assessment (DPIA) for the CCTV system

3. ACCESS AND SHARING OF DATA

3.1 GDPR Data Subject Access

CCTV footage or images may be requested as part of a Subject Access Request and according to the school's data protection policy and procedures. If footage is requested, the relevant data should be flagged on the system to prevent data being deleted in accordance with the standard retention policy.

3.2 Freedom of Information Act 2000

CCTV footage or images may be requested under the Freedom of Information Act, subject to the exemptions in the Act. If footage is requested, the relevant data should be flagged on the system to prevent data being deleted in accordance with the standard retention policy.

3.3 Requests from the police

Where CCTV footage or images are requested from by the police in order to fulfil the purposes of the system, the school will require the police to provide the required form to ensure compliant sharing. A record of the sharing of data will be maintained. If footage is requested, the relevant data should be flagged on the system to prevent data being deleted in accordance with the standard retention policy.

4. GOVERNANCE AND REVIEW

4.1 Approval and review

The Headteacher is responsible for approving this policy and monitoring its implementation. This policy will be reviewed as appropriate, and at least every three years.

5. VERSION CONTROL

Version	Author	Comments
0.1	Information Governance Manager Naomi Korn Associates	Initial draft

The School's Data Protection Officer is
Naomi Korn Associates

Sue White - Senior Data Protection Advisor

Tel: 0245 824007
Email: IG@connectix.co.uk