Policy for Data Protection and Freedom of Information

Columbia Primary School

1 DATA PROTECTION 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 Z6080460. 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 Headteacher 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

Headteacher 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

See Appendix B, data rights request procedure.

9 Personal data breaches

The school will ensure it has an agreed procedure (see Appendix A) 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 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.

18 Freedom of information policy

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

The 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 [LINK] where it proactively publishes certain types of information in a framework set by the Information Commissioner's Office.

19 How we manage requests

FOIA requests should be submitted to

If staff directly receive a request quoting Freedom of Information or the Environmental Information Regulations, they will forward it to admin@columbia.towerhamlets.sch.uk as soon as they can.

19.1 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 restarts at the beginning when clarification is received.

19.2 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.

19.3 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.

19.4 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.

Signed and dated on Governor Hub.
Approved in March 2023 by the Governing Body of Columbia School.
To be reviewed in March 2024 unless any statutory documentation is published which supersedes this policy.

VERSION CONTROL

Version	Author	Comments
0.1	Senior Data Protection Advisor, Naomi Korn Associates Ltd	Initial draft updating previous Information Governance policy

20 Appendix A – personal Data Breach Procedure

As a data controller, Columbia Primary School is bound by the UK GDPR Article 33, which requires data breaches resulting in a high risk to data subjects to be reported to the Information Commissioner's Office and Article 34, which covers the notification to data subjects affected by the data breach.

Data breach incidents include the following situations:

- Emailing or posting or sharing personal information to the wrong recipient
- Making information available by posting it on a website or social media
- Storing information in an area that lacks access controls (physical or electronic)
- Successful cyber attack or phishing attempt on the school network
- USB stick, laptop or phone containing personal data being lost or stolen
- A third-party provider notifies the school it has suffered a breach of the data it processes on the school's behalf

Procedure

The following procedure is referenced in the school's Data Protection Policy and sets the steps required by the school in managing a personal data breach.

20.1 Assessing the incident

If a data breach is suspected, please notify the Data Protection Officer as soon as possible on IG@connetix.co.uk

This may include where they have caused the breach or been notified by a supplier or a data subject.

The member of staff should provide as much information as possible to the Data Protection Officer:

- when it occurred
- all data fields or types of data lost
- who and how many data subjects are affected
- any steps undertaken

If a supplier or processor is involved, the Data Protection Officer will require the school's contract manager for that supplier to retrieve a copy of contract with the relevant breach terms and obligations.

20.2 Notifying the ICO

Where the breach will result in a high risk to the individuals affected, the school is required to notify the Information Commissioner's Office within 72 hours of becoming aware of the breach. Not all data breaches will reach the threshold for notification. The Data Protection Officer will advise the school on notification, taking into account the nature of the data involved, the risk to individuals and the potential consequences of the incident.

20.3 Notifying data subjects

There is no statutory timescale for notifying data subjects affected by a breach, but the GDPR states that, if required, notification will be carried out 'without undue delay'. The Data Protection Officer will advise the school on whether to contact data subjects,

20.4 After the breach

In the aftermath of a breach there will be immediate measures the school should take such as:

- contacting an unauthorised recipient
- retrieving or deleting a mis-sent email
- taking down a hacked website

There will be a number of longer-term remedial measures that a breach may highlight:

- training
- security review
- new procedures
- amending risk registers

These measures will be advised by the DPO and will be managed by the school

20.5 Record keeping

The following information will be kept to record breaches:

- Log of incidents, including date, summary and outcome
- Case file of the incident, including ICO correspondence, data subject correspondence and record of Incident Group actions

Please see the sample data breach record form in Section 7.

21 Appendix B - Data Rights Request Procedure

The UK GDPR includes a range of rights for individuals (hereafter 'data subjects' as in the language of the law) around their data. Anyone whose data is processed by the school can make a rights request. The rights are not absolute, and a number of restrictions apply in certain circumstances.

The following procedure is referenced in the school's Data Protection Policy and sets out the requirements for dealing with rights requests.

If you have received a rights request in writing or verbally, please notify the Data Protection Officer as soon as possible on IG@connetix.co.uk

21.1 Requests on behalf of a data subject

A data subject may have a solicitor or other third party make a request on their behalf. In these circumstances the school should ensure that there is proof of the authority being given by the data subject (e.g., a signed form).

21.2 Verifying the identity of the requester

The school may need to request specific information from the individual to confirm their identity and ensure their right to access the information (or to exercise any of their other rights). This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it. The information the school requires should be reasonable and proportionate. In some cases it may be appropriate to request a formal identification document, in other cases a username or login credentials may be sufficient.

21.3 SARs from pupils

Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The school must, however, be satisfied that the child or young person lacks sufficient understanding; and the request made on behalf of the child or young person is in their interests.

21.4 Timescales

The school has 30 days to respond to the request. In circumstances where the request is particularly complex, you may extend this time to 90 days. If you do this, you must inform the data subject within 30 days of the original request.

21.5 Refusing a request

The school can refuse to comply with a request if it is

- Manifestly unfounded, i.e., malicious, disruptive or targets a specific member of staff)
- Excessive, i.e., will create a large burden on resources or is a repeat / overlapping request with others from the same individual

With both of the grounds for refusal, it is quite a high threshold to reach and the school would need to record how this threshold was reached in the event of an appeal. If the request is excessive, it may be possible to charge a fee (see below).

21.6 Charges

In most cases, a data subject rights request is free. If, in exceptional circumstances, the request will take excessive resource to comply with, the school may consider a fee. This can include costs such as printing, equipment (such as disks or USB sticks) and staff time. The school should record a breakdown of how these costs are calculated.

21.7 Redaction

In the right of access, the data subject only has the right to receive a copy of their personal data. Any redactions should be added to a document to ensure other people's data is not disclosed. Redaction software is available on applications such as PDF. Always ensure that redactions cannot be read through (for example if carried with a marker pen) or undone (if carried out on a word processing programme). If redaction is difficult, you may consider extracting information into a new document.

21.8 Reasonable adjustments

The school has an obligation under the Equality Act 2010 to make a reasonable adjustment for data subjects with disabilities. It is, for example, unacceptable to provide PDF scans of documents without optical character recognition to a data subject who requires a screen reader to access information. The school should check with the data subject if they have any special requirements for accessing the data.

21.9 Secure sending / sharing

Disclosing the response to a subject access request requires the same commitment to data security as the other processing the school carries out. To ensure the secure transfer or sharing of the response, the school will:

- provide the responses in electronic format, unless the data subject makes a reasonable request for the data in hard copy
- double check all contact details for accuracy before dispatch or pressing send
- if providing the data via email the school should ensure that all attachments are password protected, with the password be communicated to the data subject in a separate communication, such as an email or phone call
- if providing the data by post the school will use registered delivery
- if providing remote access to the information for the data subject, the school will ensure controls are in place about how access is granted and for how long