



UNIVERSITY OF
CAMBRIDGE
PRIMARY SCHOOL

Data Protection Policy

Approved by
Finance Committee

Last reviewed on
May 2019

Next review due
May 2022



**RELEASING THE
IMAGINATION:
CELEBRATING
THE ART OF
THE POSSIBLE**



Introduction

This policy applies to all employees, workers and contractors.

The Governing Body/Trustees of University of Cambridge Primary School are committed to processing personal data (which may be held on paper, electronically, or otherwise) about our employees and we recognise the need to treat it in an appropriate and lawful manner, in accordance with the General Data Protection Regulation (GDPR). The purpose of this policy is to set out the principles by which we will handle your personal data.

Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action, including dismissal.

The schools Designated Data Protection Lead's and Designated Data Protection Officer are responsible for ensuring compliance with the GDPR and this policy. Any questions about the operation of this policy or concerns that there has been a breach of this policy should be referred in the first instance to Amy White or James Biddulph (School's Designated Data Protection Lead)

Responsibilities

The Governing Body/Trustees must:

manage and process personal data properly;

protect the individual's rights to privacy;

provide an individual with access to all personal information held on them.

The Governing Body/Trustees have a legal responsibility to comply with the law, including the General Data Protection Regulation. The individual with overall responsibility for this policy is the Designated Data Protection Officer.

The Governing Body/Trustees are required to notify the Information Commissioner of the processing of personal data; this is included in a public register. The public register of data controllers is available on the Information Commissioner's website.

The Governing Body/Trustees' Designated Data Protection Officer is responsible for drawing up guidance on good data protection practice and promoting compliance with the guidance through advising employees on the creation, maintenance, storage and retention of their records which contain personal information.

Every employee that holds, or has access to, information about identifiable living individuals must comply with data protection legislation in managing that information. All employees are responsible for acting in accordance with the policies, procedures and guidelines and within the provisions of the General Data Protection Regulation. Individuals may be liable for breaches of the Regulation.

Definitions

In this policy, unless otherwise stated or unless the context otherwise requires, each term will have the meaning set out below:

Data protection means practices and operations relating to the fair and lawful treatment of Personal Data and an understanding of the regulatory requirements relating to data privacy.

Personal data is data which relates to a living individual who can be identified:

from this data; or

from this data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Examples of personal data can include, but are not limited to:

names

addresses

telephone numbers

dates of birth

National Insurance numbers

employee numbers

named email addresses

account details

CCTV images

photographs

personal opinions

internet browsing history

static/dynamic IP addresses

Special Categories of personal data (also known as sensitive personal data) includes:

racial or ethnic origin;

political opinions;

religious or philosophical beliefs;

trade union membership;

the processing of genetic data;

biometric data for uniquely identifying an individual;

data concerning health or data concerning an individual's sex life;

sexual orientation;

medical information.

Additionally, although not sensitive under data protection legislation, financial data and information relating to criminal convictions should also be treated with additional safeguards due to their associated risks.

Data processing in relation to information or data, means obtaining, recording or holding the information/data or carrying out any operation or set of operations on the information/data, including:

organisation, adaptation or alteration of the information/data;

retrieval, consultation or use of the information/data;

disclosure of the information or data by transmission, dissemination or otherwise making available;

alignment, combination, blocking, erasure or destruction of the information or data; or

storage of information or data, whether electronically or manually (paper based).

Data subject an individual who is the subject of personal data.

Data controller means a person or organisation who (either alone or jointly or in common with other persons) determines the purposes for which and the way any personal data is, or is to be, processed.

Data processor in relation to personal data, means any person or organisation (other than an employee of the data controller) who processes the data on behalf of the data controller.

Relevant filing system means any paper-based records which are structured in a way which is either:

By reference to the individual by name or code;

By reference to criteria relating to individuals.

Obtaining Information

The organisation will process data about employees for legal, administrative and management purposes and to enable us to meet our legal obligations as an employer, for example to pay you, monitor your performance and to confer benefits in connection with your employment.

The organisation may process sensitive personal data relating to employees including, as appropriate:

- a) information about an employee's physical or mental health or condition in order to monitor sickness absence and take decisions as to the employee's fitness for work;
- b) the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- c) in order to comply with legal requirements and obligations to third parties.

Principles relating to processing of personal data

In line with GDPR, anyone processing personal data must comply with the following principles. It is our policy that personal data must be:

- a) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation');
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay ('accuracy');
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

The Governing Body/Trustees shall be responsible for, and must be able to demonstrate compliance with, these principles.

Purposes of Information and Length of Time Retained

Personal data will be held in accordance with the Governing Body/Trustees' Policy on Retention of Personal Information. We will not keep personal data longer than necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

The Governing Body/Trustees will state the purposes for which it holds personal information, and will register with the Data Protection Commissioner all the purposes for which it processes personal data.

Nature of Information

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

Disclosure of Information

Personal data will be used only for the purpose for which it was gathered, unless the consent of the data subject concerned has been obtained to a new or varied use.

Routine disclosures will be specified on the Data Protection register and in the organisation's own Data Protection publication scheme and consent will be deemed to have been given to routine disclosures so included.

In other cases the explicit consent of the data subject will be obtained in writing. Confirmation of consent by telephone is acceptable if a written request has been received which implies the consent of the data subject.

Access to personal data will be refused if the data user is uncertain whether the person requesting access, including another employee, is entitled to it. In such a case, the request must be referred to the Data Officer for consideration before the request is rejected.

Data Breach

If we discover that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, the Data Protection Officer will report it to the Information Commissioner within 72 hours of discovery.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, all affected individuals will be informed of the breach and provided with information including the type of data and likely consequences of the breach, plus mitigating steps taken.

Any breach of the policy will be fully investigated and remedial steps taken to ensure a similar breach cannot happen again.

A record of all data breaches, regardless of their size or effect, will be retained within the Breach Register, as set out in Appendix 1 of this Policy, available from the Schools Designated Data Protection Lead's.

Individual rights

As a data subject, individuals have a number of rights in relation to their personal data.

Subject access requests

Individuals have the right to make a subject access request. If an individual makes a subject access request, the organisation will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and

- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making.

The organisation will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

If the individual requests additional copies, the organisation reserves the right to charge a fee, which will be based on the administrative cost to the organisation of providing the additional copies.

To make a subject access request, the individual should send the request to dataprotection@universityprimaryschool.org.uk. In some cases, the University of Cambridge Primary School may need to ask for proof of identification before the request can be processed. The University of Cambridge Primary School will inform the individual if it needs to verify their identity and the documents it requires. The individual will need to complete a Subject Access Request Form as set out in Appendix 2.

The University of Cambridge Primary School will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the University of Cambridge Primary School processes large amounts of the individual's data, it may respond within three months of the date the request is received. The University of Cambridge Primary School will write to the individual within one month of receiving the original request to tell them if this is the case.

If a subject access request is manifestly unfounded or excessive, the University of Cambridge Primary School is not obliged to comply with it. Alternatively, the University of Cambridge Primary School can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request to which the University of Cambridge Primary School has already responded. If an individual submits a request that is unfounded or excessive, the University of Cambridge Primary School will notify them that this is the case and whether or not it will respond to it.

Other rights

Individuals have a number of other rights in relation to their personal data. They can require the University of Cambridge Primary School to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the University of Cambridge Primary School's legitimate grounds for processing data (where the University of Cambridge Primary School relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and

- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the University of Cambridge Primary School's legitimate grounds for processing data.

To ask the University of Cambridge Primary School to take any of these steps, the individual should send the request to dataprotection@universityprimaryschool.org.uk

Access to Personal Files

Employees are entitled to know if the organisation holds information about them. Any request for information must be made formally in writing addressed to Amy White or James Biddulph School's Designated Data Protection Lead's

Data Security and Impact Assessment

The University of Cambridge Primary School will determine and maintain an appropriate level of security (and back-up) for its premises, equipment, network, programs, data and documentation, and will ensure that access to them is restricted to appropriate individuals. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

Monitoring Activities

The University of Cambridge Primary School will record and monitor usage of all company IT equipment, user activity, voice traffic, email and internet usage as deemed necessary.

Those responsible for undertaking the monitoring will observe the strictest confidentiality when undertaking these activities. The report will be made directly to Amy White or James Biddulph School's Designated Data Protection Lead's , who will determine any action that may need to be taken.

Monitoring of IT equipment, electronic data, telephone calls, emails, internet access, network access and remote organisation's policies, procedures and guidelines.

Request for Data by Public Authorities

Requests for personal data may come from public authorities, including but not limited to the following:

the Police;

the Department of Work and Pensions;

the UK Border Agency;

HM Revenue & Customs;

Local Authorities;

DVLA.

Requests received from a public authority will only be processed when submitted in writing, including electronic communication. Such requests for data usually require that the University of Cambridge Primary School does not inform, or gather consent from, the data subject when responding to the request. When a request is received, this should first be referred to the School's Designated Data Protection Lead who will ensure that the request is valid.

Data can only be disclosed without the knowledge and consent of the data subject where it is processed for either the:

prevention or detection of crime;

apprehension or prosecution of offenders; or

assessment or collection of tax or duty.

Additionally, it must be shown that informing or gathering consent from the data subject would likely prejudice the crime or taxation purposes.

Where these conditions are not met, the Designated Data Protection Lead's may decide to not disclose the data. Where the Designated Data Protection Lead decides the records should not be disclosed or only partially disclosed, they must record in writing their reasons. A public authority may have a Court Order issued for the disclosure of documents. Any objections should be recorded along with the Court Order however the data should be disclosed.

Training

All new and existing employees who handle personal data will receive training on data protection procedures, which includes information about the standards the organisation expects its employees to observe in the use of personal data.

References

The Governing Body/Trustees will comply with DfE guidance on references as amended from time to time, in particular in relation to safeguarding children and safer recruitment in education.

Review of Policy

This policy shall be reviewed as necessary. We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail, email and/or staff notice board.

Other related documents:

This policy is supported by the following documents *[to be amended to reflect internal policies in place however may include]*:

- *How Staff Handle Data*
- *IT Acceptable Use Policy*
- *Privacy Notices*
- *Data Retention Policy*
- *Code of Conduct/Disciplinary Policy*

Relevant Contacts:

Data Protection Officer

Please refer any queries, issues or requests received to the School's Designated Data Protection Lead's:

Dr James Biddulph and Miss Amy White

01223 792440

School's Designated Data Protection Officer

Mr James Knapton

01223 332331

ICO contact details

If you require more information about the General Data Protection Regulation, the Data Protection Bill, or are unhappy with the way *[name]* has dealt with your data please contact:

The Information Commissioner

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

www.ico.org.uk

Appendix A

Example of Breach Register

Breach Ref No:	Breach:	Details:	Severity:	Actions:	Reported to Data Subject Y/N	Actioned by:
1:						
2:						
3:						
4:						
5:						
6:						
7:						
8:						
9:						
10:						
11:						
12:						
13:						

Appendix B

SUBJECT ACCESS REQUEST FORM

You should complete this form if you want the University of Cambridge Primary School to supply you with a copy of any personal data which we hold about you.

We will endeavour to respond promptly and in any event within 30 days of the arrival of the latest of the following:

- Our receipt of this request; or
- Our receipt of any further information we request from you, which is required to enable us to comply with your request.

SECTION 1 - Details of the person requesting the information

Full name:
Address:
Tel No:
Email address:

The Information supplied in this form will be used only for the purposes of identifying the personal data you are requesting.

SECTION 2

Are you the data subject?

Yes	No
-----	----

Please tick appropriate box and read the instructions which follow it.

YES: If you are the data subject please supply evidence of your identity, i.e. a driving license, passport, national identity card, a recent letter or bill from a utility company as evidence of address, and a stamped addressed envelope for returning the document – now please go to section 4)

NO: Are you acting on behalf of the data subject with their written authority? If so, that authority must be enclosed. You must supply evidence of your identity and the identity of the data subject, i.e. a driving license, passport, national identity card, a recent letter or bill from a utility company as evidence of address, and a stamped addressed envelope for returning the document now please go to section 3)

If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request

SECTION 5

If you wish to receive information about the following, please tick the boxes:

Why we are processing your personal data	
To whom your personal data are disclosed (if any)	
The source of your personal data	

NOTES

If the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances we may not be able to disclose the information to you, in which case you will be informed promptly.

Please note that, while in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 14 (5) b of the GDPR, not to provide you with copies of information requested if to do so would take “disproportionate effort”. However we will make every effort to provide you with a satisfactory form of access or summary of information if suitable. If further copies are requested, we may charge a reasonable fee based on administration costs as stated in Article 15 (3).

DECLARATION

Please note that any attempt to mislead may result in prosecution.

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application to the University of Cambridge Primary School is true. I understand that it is necessary for the University of Cambridge Primary School to confirm my/ the data subject’s identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed..... Date

Documents which must accompany this application:

- Evidence of your identity (section2)
- Evidence of the data subject’s identity (if you are applying on behalf of someone else)
- Authorisation from the data subject to act on their behalf (if applicable)
- Stamped addressed envelope for return of proof of identity/authority documents.
- When you have received the requested information if you believe that:
 - The information is inaccurate or out of date; or
 - We should no longer be holding that information; or
 - We are using your information for a purpose of which you were unaware;
 - We may have passed inaccurate information about you to someone else;
- then you should notify our Data Protection Officer at once, at the address below.

Please return the completed form to :

Designated Data Protection Lead, University of Cambridge Primary School, Eddington Avenue, Cambridge CB3 0QZ