Coulsdon C of E Primary School

Data Protection Policy (GDPR)

November 2023 (next review November 2024)

The ethos of this school is to enable every child to learn and develop in a Christian environment. We ask all parents of whatever faith applying for a place here to recognise and support this ethos and its importance to the school

Together, growing in mind, body and spirit

Contents

1. What is the purpose of this policy?

Under data protection legislation, Coulsdon C of E Primary School (the School) is the data controller of the personal information we hold. The School designates the Head Teacher as its representative regarding the protection of data.

The postal address of the school is: Coulsdon C of E Primary School, Bradmore Green, Old Coulsdon, Surrey, CR5 1ED. For queries, please contact the school office on 01737 554 789 or by email to office@ccofe.uk

The School is required to keep and process personal information about its pupils, families and staff in accordance with its legal obligations. This information will be processed in accordance with the EU General Data Protection Regulation 2018 (GDPR).

The school may, from time to time, be required to share personal information with other organisations, including the Local Authority (LA), Department for Education (DfE,), Southwark Diocese Board of Education (SDBE), other schools, and relevant bodies that provide services to the school.

This policy will outline the legal framework, practices and processes used in the school with regards to the proper collection, processing and retention of personal data we hold.

A summary of this Data Protection Policy is provided in our Privacy Notices which can be downloaded from The School website www.coulsdoncofe.co.uk or are available on request from the school office.

This document is a working document and will be regularly updated, (at least once per year) to reflect changes in the working practices of the school. Please ensure that you access the most recent version of this document either through the website or by contacting the school office.

2. Why do we collect and use data?

Coulsdon C of E Primary School is a voluntary aided maintained school. The school is a publicly funded body responsible for providing state education for children. The school is required by law to comply with legislation including, but not limited to, the following:

- The Education (Pupil Information) (England) Regulations 2005 (amended 2016)
- The School Standards and Framework Act 1998
- The General Data Protection Regulation 2018 (GDPR)
- The Freedom of Information Act 2000
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004

This policy will underpin all data processing activities within the school and makes reference to the following other school policies:

- Acceptable Use Policy
- E-Safety Policy
- Information Governance Procedures
- Freedom of Information Policy

The school uses the information it holds in order to:

- Support the teaching and learning of pupils and staff
- Monitor and report on progress and achievement
- Provide appropriate care and safeguarding for pupils and staff
- Assess the quality of our service
- Comply with our legal obligations

3. What data is covered by this policy?

The school recognises the following categories of data which are collected and processed by the school. This policy applies to both personal data held electronically and data stored in paper records in our filing systems. Personal data may be processed according to specific criteria, including chronologically ordered data and data which has been pseudonymised.

Personal data is information that relates to an identifiable, living individual, this can include information relating to online identity such as usernames or IP addresses.

Sensitive personal data is defined as a special category of personal data (refer to GDPR Article 9). This can include the processing of genetic data, biometric data and data concerning health matters. The School applies additional measures to protect and secure this type of data.

Criminal convictions and offences are another example of personal data, but which are not included under the category of sensitive personal data. The School applies additional safeguards to the processing of this data (refer to GDPR Article 10).

4. What are the key principles and lawful reasons used to process data?

The school will ensure that all personal data is only ever collected, processed and stored according to the key principles identified in the GDPR to ensure that privacy and data security is embedded within the culture of the organisation at all levels. The school recognises that personal data may only be processed lawfully, the lawful reasons used by the school are identified as follows:

- To allow the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller to carry out the duties of the school
- To protect the vital interests, health or wellbeing of an individual
- To comply with legal obligations
- To deliver a contract, or to take steps required to enter in to a contract
- To undertake other legitimate interests pursued by the Data Controller or a third party
- With the consent of the person concerned, which has been legally obtained

5. What personal data is collected?

The school can collect and process the following personal data relating to pupils or their families:

- Personal information – e.g. names, addresses, date of birth
- Characteristics including ethnicity, language, nationality, country of birth, religion, free school meal eligibility and photographs for identification
- Attendance information including absences and absence reasons

- Assessment information including National Curriculum assessment results and scores used to measure learning, development and progress
- Medical history and information relevant to health & wellbeing such as allergy information
- Information relating to identified Special Educational Need & Disability (SEND)
- Behavioural information including exclusions and incident reports
- Safeguarding information relating to protecting the safety or best interest of children including care and social services data, legal or judicial communications and information supplied by related agencies

The school can collect and process the following personal data relating to its employees and governors:

- Personal information – e.g. names, addresses, date of birth
- Characteristics including ethnicity, language, nationality, country of birth and photographs for identification
- Attendance information including absences and absence reasons
- Employment & Contractual information such as qualifications, criminal records checks, references, employment history, trade union membership, religion and financial data such as bank details & tax information
- Medical history and information relevant to health & wellbeing such as disability or allergy information
- Performance Management information such as appraisals or disciplinary records

The school can collect and process the following personal data relating to contractors and visitors:

- Personal information – e.g. names, addresses, date of birth
- Characteristics including ethnicity, language, nationality, country of birth and photographs for identification
- Employment & Contractual information such as qualifications, criminal records checks, references, employment history, trade union membership, religion and financial data such as bank details & tax information

6. What is meant by obtaining lawful consent?

The school may identify additional uses of your data, which may be of benefit to your child or the school community. Examples may include optional extra-curricular activities, fundraising or promotional activities. We will always seek your consent before using your data for these reasons. If you give consent, you may change your mind at any time.

Processes for obtaining consents are admission application forms and supplementary information forms and the new parents pack completed when joining the school. Permission may be withdrawn at any time by informing the school office.

7. Will personal data be shared?

The school is legally obliged to share data about pupils and staff with the Department for Education (DfE). The DfE uses this data for school funding and educational attainment policy and monitoring.

The DfE routinely requests data throughout the year which include the School Census return and Early Years Census. To find out more about the pupil information we share with the DfE for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Some of this information is then stored on the National Pupil Database (NPD), which is permitted in law by the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD please go to: https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

The DfE may share information about pupils from the NDP with third parties who promote the education or wellbeing of children through research, providing information, advice or guidance.

To find out more about information about the DfE's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

The school will also share personal data with approved third parties or contractors in order to deliver its aims.

- Department for Education (DfE)
- Southwark Board of Education
- Health and SEND Professionals
- Service Suppliers
- Payroll Providers, Pension Bodies, Auditors
- Pension Bodies
- Other Schools

The information shared may include sensitive personal information such as information about health, special educational needs, or disabilities. This information is used to provide the correct services to support children, families or employees and is only shared on a strictly need to know basis in full compliance with individual's rights.

The school is required by law to check the identity and Criminal Record of all employees, governors and volunteers in order to safeguard children and staff.

The school will conduct checks using the Disclosure and Barring Service (DBS). In order to carry out these checks, it is required for authorised persons to share sensitive personal data with the DBS.

Personal Data will be processed by the DBS and the results of this processing provided to the school. You may review the privacy notices provided by the DBS for further information on the gov.uk website.

https://www.gov.uk/government/organisations/disclosure-and-barring-service

8. How do we use photography and video?

The school recognises that the recording of images of identifiable individuals is a form of processing personal information which must be carried out in line with data protection requirements.

The school makes use of CCTV systems in order to provide enhanced security of the premises and to better safeguard the interests of pupils & staff.

- The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.
- The school notifies all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
- Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- All CCTV footage will be kept for 31 days for security purposes; the Head Teacher, Office Administrator and SBM are responsible for keeping the records secure and allowing access.

The school captures photographs of pupils, staff, contractors and visitors to our site for the purposes of identification and authorisation of access. These images may be further processed and linked to other information we hold such as emergency medical needs, or attendance records.

The school may use photography and video images for other explicit purposes in order to deliver its aims. Full details of these purposes are outlined in our policy below.

- The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.
- If the school wishes to use images/video footage of pupils in a publication, such as the school website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.
- Precautions, as outlined in the Photography at School Events Policy, are taken when publishing photographs of pupils, in print, video or on the school website.
- Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

9. Will personal data be published?

The school will not publish any personal data, including photos or images, in a public forum either online or in print without obtaining explicit consent in advance.

10. How long is personal data stored for?

Personal data held by the school is stored and deleted according to our Data Retention Policy.

Personal data is not kept on a permanent basis and is only stored for as long as is necessary to fulfil its intended purpose. Personal data is deleted when it is no longer required. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also for example to enable the provision of references.

Paper documents will be shredded or securely disposed of, and electronic data scrubbed clean or permanently erased once the data is no longer required.

Please review our Data Retention Policy for further details of specific data items and their retention schedules.

11. Who is accountable for data protection?

Under data protection legislation, the school is the Data Controller of the personal data we hold.

The GDPR requires that the Data Controller shall be responsible for, and able to demonstrate, compliance with the principles outlined above. The School designates the Head Teacher as its representative with regards to data protection.

As a publicly funded body the Data Controller is required to appoint a Data Protection Officer (DPO).

The School has appointed OpenAIR Systems Limited as its DPO. The DPO can be contacted by email dataprotection@openair.systems or in writing to OpenAIR Systems, 1 Holmbury Grove, Featherbed Lane, Croydon, Surrey, CR0 9AN
The DPO has a range of responsibilities which support the school in meeting its obligations under GDPR. The DPO will act as a point of contact and adviser to the school, its employees and clients.

12. How is personal data processed and protected?

The school ensures appropriate technical measures and processes are in place to protect data and privacy of individuals. The school defines comprehensive, understandable and transparent policies which give due regard to the protection & security of data. Policies underpin the culture and behaviours adopted by the school and outline our business processes and structure. All policies are reviewed on a regular basis to ensure they reflect the most up to date circumstances and any changes in working practice. When reviewed, all policies are checked alongside this data protection policy to ensure a comprehensive and integrated approach to privacy is delivered.

The school maintains a Data Protection Audit as an internal record of all data processing activities carried out, and reviewed at least once per year to ensure the content is kept up to date. The audit includes full itemised details of each data processing activity, nature & categories of data, reasons for processing and the systems used to carry out the processing.

When introducing new systems or new ways of processing personal data, the school will conduct a Data Protection Impact Assessment (DPIA) in order to ensure proper integration and compliance with the law and our policies. Any new systems implemented by the school will ensure data protection is implemented by design and privacy enabled by default.

In order to ensure that data is protected, the school has identified the following measures which are implemented to minimise the risks involved in processing and storing information:

At School

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

- Confidential paper records will not be left unattended or in clear view anywhere with general access.
- Paper copies containing personal information will be shredded when no longer needed
- Personal data should be stored on a School shared drive or electronic document management systems wherever possible and not held on a portable computer device.
- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Information on shared drives or electronic document management systems should only be stored in areas with appropriate access permissions, i.e., access is restricted to only those who have a need to view it.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff and governors will only use their personal laptops or computers for school purposes if they are password protected and they are accessing the Google Drive. Personal data must only be stored on school devices
- All necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Personal files will not be sent out by normal post. Postal and email addresses will be checked carefully to ensure safe dispatch of information

Out of school:

- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Where personal information needs to be transported away from School offices this should, wherever possible, be done on secure portable computing devices (i.e. encrypted School laptops) and not as paper documents.
- Paper based information and laptops will be kept safe, secure and close to hand and never unattended when taken out of school.
- Removal of personal paper based information will only be for short periods and will be returned when the user is next in the office to be filed or shredded. When transferring paper based information by car, it is placed in the boot and is kept locked.
- Portable computing devices used for remote working must be secure and comply with School ICT Security policies. This includes laptops. Information classified as personal data or sensitive personal data will not be stored on non-School owned devices.
- Any employee who chooses to undertake work using their own personal IT equipment is not permitted to hold any database, or carry out any processing of personal or sensitive personal data relating to the School's employees, or customers.
- If paper based information or portable computer devices are lost or stolen then the loss must be reported to the Head Teacher immediately.

- Confidential or sensitive work matters will not be discussed where people who should not have access to the information may overhear e.g. in communal areas in the workplace or outside work.

Sharing data

- Personal information should not be emailed to or auto forwarded to a private non-School email address. Secure email must be used to send personal information outside of the School network.
- Before sharing data, all staff members will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
- The physical security of the school's buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- Coulsdon C of E Primary School takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.
- The Head Teacher is responsible for continuity and recovery measures are in place to ensure the security of protected data.

13. What are your rights regarding your personal data?

The school recognises the rights of individuals with regards to our use of their personal data, a list of your rights are as follows:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

The school will ensure that these rights are respected by ensuring that all our policies and processes regarding data processing and data storage are compatible with these rights.

In addition to the rights detailed above, individuals have further rights relating to the automated processing of their personal data.

The school does not make use of any automated decision making in the processing of data, neither does it undertake automated profiling of individuals.

14. What happens when there is a breach of your privacy?

The school will use practical & technical measures to protect personal data from loss or any other unauthorised alteration, disclosure, or access.

In the event of a breach of privacy as described above, the Head Teacher in consultation with the DPO, will take the following action:

- Assess the nature of the personal data breach, including the categories of data concerned and approximate number of individuals and records affected
- Identify if the breach is likely to result in any risk to the rights and freedoms of individuals. Risk of the breach having a detrimental effect on individuals, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis
- Report all notifiable breaches to the Information Commissioner's Office within 72 hours of the school becoming aware of it
- If a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those individuals concerned directly and without undue delay
- In the case of breaches deemed to be low risk, further training will be considered for individuals or the whole school team

Both the school and individuals may be liable for breaches of the Regulation. Each school will have a 'Breach Log' to monitor and record any breaches. Failure to report a breach to the ICO when required to do so may result in a fine, as well as a fine for the breach itself. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the DPO will inform the police of the security breach.

15. How do you request access to view your personal data?

Under data protection legislation, any individual about whom the school processes personal data (the Data Subject) has the right to request access to view the information that we hold about them.

Requests for access to your personal information must be recorded in writing; this is known as a Subject Access Request (SAR).

You may make a request verbally by speaking to a member of staff who will record your request.

Alternatively, you may use our Subject Access Request Form or write your own letter addressed to the Head Teacher sent care of our nominated DPO; OpenAIR Systems,1 Holmbury Grove, Featherbed Lane, Croydon, Surrey, CR0 9AN, or submit an emailed a request to coulsdoncofe.sars@openair.systems

You will receive an automated acknowledgement of the receipt of your request when sent via email. All SAR requests will be processed in accordance with GDPR requirements.

16. How do you raise a concern about the way we process personal data

If you have a concern about the way we collect or use your personal data, we invite you to raise the matter with us in the first instance, either by contacting the school, or via our DPO.

Alternatively, you can contact the Information Commissioner's Office:

By post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

By telephone: 0303 123 113 or 01625 545 745

Online: https://ico.org.uk/concerns

17. Consequences of a Breach

A GDPR breach can have serious consequences for both the school and its staff. If a school fails to comply with GDPR regulations, it can face fines of up to 4% of its global annual revenue or €20 million, whichever is greater. In addition to the financial penalties, a GDPR breach can also result in reputational damage, loss of trust from parents and students, and legal action from affected individuals. It is crucial that all staff members understand the importance of GDPR compliance and take appropriate measures to protect personal data. Staff members who are found to be responsible for a breach may face disciplinary action, which may include termination of employment.

18. When will this policy be updated?

This policy will be reviewed at least once per year by the school.

This policy is a working document and can be updated to reflect changes in the working practices of the school at any time. Please ensure that you access the most recent version of this document either by downloading the current version from the website or by contacting the school office.

The next scheduled review date for this policy is November 2024.

Malcolm Bulbeck
Chair of Finance and Premises Committee
21st November 2023

Paul Garratty

Coulsdon C of E Headteacher

21st November 2023