*Doing our best to achieve our best*

# Clarendon Primary School, Nursery & Family Centre
# Data Protection Policy

## 1. Introduction and Purpose of Policy

The purpose of this policy is to provide information about our approach to collecting and using personal data in the course of our day-to-day work as well as the rights available to those whose data we hold. It aims to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 as set out in the Data Protection Bill.

It applies to personal data we collect both as an employer and as an education provider, such as that contained within pupil and staff records as well as information we hold on parents, governors, volunteers, visitors and other individuals with whom we interact. It also applies to all personal data whether in a paper or electronic format.

## 2. Policy Statement

The Governing Body is committed to ensuring that personal data is collected and used in a way which is transparent, clearly understood and meets minimum legal requirements and best practice guidance. They recognise the need for individuals to feel confident that their data is used only for the purposes that they have been made aware of, and that it is stored securely and for no longer than is necessary. As part of this commitment, we want to ensure that individuals understand the rights available to them if they want to question or raise concerns about the way their data is being processed.

The school has appointed a Data Protection Officer whose role is to monitor internal compliance, including with this policy, to inform and advise on data protection obligations and act as a contact point for individuals and the Information Commissioner's Office.

## 3. Legislation and guidance

This policy has been written to meet the requirements of GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) and the ICO's code of practice for subject access requests.

In addition, this policy also complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

## 3. Definitions

| Term | Definition |
|---|---|
| **Personal data** | Any information relating to an identified, or identifiable, living individual.<br><br>This may include the individual's:<br>• Name (including initials)<br>• Identification number<br>• Location data<br>• Online identifier, such as a username<br><br>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. |

| | |
|---|---|
| **Special categories of personal data** | Personal data which is more sensitive and so needs more protection, including information about an individual's:<br><br>• Racial or ethnic origin<br>• Political opinions<br>• Religious or philosophical beliefs<br>• Trade union membership<br>• Genetics<br>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes<br>• Health – physical or mental<br>• Sex life or sexual orientation |
| **Processing** | Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.<br><br>Processing can be automated or manual. |
| **Data subject** | The identified or identifiable individual whose personal data is held or processed. |
| **Data controller** | A person or organisation that determines the purposes and the means of processing of personal data. |
| **Data processor** | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller. |
| **Personal data breach** | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. |

## 4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others and is therefore a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5a. Expectations of staff

We expect all staff working for or on behalf of the school, (whether employees, casual workers, supply staff, volunteers or consultants,) to recognise and adhere to the high standards of data protection we uphold. Everyone has a responsibility for helping to ensure that personal data, whether their own or that of third parties, is accurate, kept up to date and held securely.

Whilst certain members of staff will be specifically collecting and processing data as part of their role, we expect all staff to adhere to the following rules:

- Only access or process personal data they are authorised to as part of their role and in accordance with the documented purposes for processing, (and not for any other purpose).
- Keep personal data confidential and only disclose it to individuals who are authorised to see it. (If in any doubt, staff should consult their line manager or the Data Protection Officer).
- Not remove personal data from its authorised location without permission and, where permission is granted, to ensure that appropriate security measures are in place whilst the data is moved or relocated.
- Not keep work-related personal data on personal devices, such as mobile phones and tablets, or on local computer hard drives or unencrypted USB sticks.
- Take responsibility for ensuring that personal passwords are strong, are changed regularly and never shared.
- Adhere to all security measures designed to keep personal data safe from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.
- Participate in training or briefings and read circulated documents aimed at increasing awareness of data protection legislation and good practice.
- Be aware of data protection issues as part of their day-to-day work, particularly as part of any new projects, and report any concerns relating to personal data, (including any potential data breaches) as a matter of urgency to the Data Protection Officer.

These rules are an integral part of the school's data security practices in order to comply with data protection legislation. As such, in accordance with the disciplinary procedure, a breach of these rules could be treated as a disciplinary offence and potentially gross misconduct,

## 5b. Specific roles and responsibilities

**5.1 Governing body**
The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

**5.2 Data protection officer**
The data protection officer, (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They report on their activities directly to the governing body and, where relevant, report to them their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Our DPO is Mrs Carol Foley and is contactable on email via dataprotection@clarendon.surrey.sch.uk

**5.3 Headteacher**
The headteacher acts as the representative of the data controller on a day-to-day basis.

**5.4 All staff**
Staff are responsible for:
- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school of any changes to their personal data, such as a change of address.
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
  - If they have any concerns that this policy is not being followed.
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way.
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual.
  - If transfer of personal data outside the European Economic Area is required. (If this is ever required, the DPO will seek advice before responding)
  - If there has been a data breach.
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals.
  - If they need help with any contracts or sharing personal data with third parties.

## 6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:
- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- Accurate and, where necessary, kept up to date.
- Kept for no longer than is necessary for the purposes for which it is processed.
- Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

## 7a. Our Approach to Processing Personal Data

We use privacy notices to inform individuals whose personal data we collect about how we use their information and the legal basis on which we are processing it. If we want to process data for new reasons in the future, we will inform affected individuals first.

We process special categories of personal data and criminal offence data, for example to meet our obligations under employment law. Where we do so, this processing is underpinned by policies on the use of such data.

For some of the data we process we rely on legitimate interests as the legal basis for processing. We do not rely on this basis unless we have first concluded that the rights and freedoms of individuals do not override those interests.

Personal data we hold on individuals is held in secure paper and/or electronic files to which only authorised personnel have access. Information is held for no longer than is deemed necessary, in accordance with our data retention schedules and privacy notices.

If we are planning to process data and this processing is likely to result in a high risk to individuals' interests, we will undertake a Data Protection Impact Assessment (DPIA) to help us identify and minimise the data protection risks.

We always aim to rectify inaccurate or out-of-date information promptly when notified and encourage anyone whose data we hold to inform us when their details have changed.

## 7b. Collecting personal data

**7b.1 Lawfulness, fairness and transparency**
We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract.
- The data needs to be processed so that the school can **comply with a legal obligation.**
- The data needs to be processed to ensure the **vital interests** of the individual are met, e.g. to protect someone's life.
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions.
- The data needs to be processed for the **legitimate interests** of the school or a third party, (provided the individual's rights and freedoms are not overridden)
- The individual, (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**.

For special categories of personal data, we will also meet at least one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018 (Article 9).

When offering online services to pupils, such as classroom apps or access to other online educational support resources, we intend to rely on consent as a basis for processing and obtain parental consent as part of our pupil registration and annual data checking processes. (**N.B.** This excludes consent for online counselling and preventive services).

**7b.2 Limitation, minimisation and accuracy**
We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data. (**I.e.** through 'Privacy Notices'.)

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before doing so, and will subsequently seek further consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the 'Information and Records Management Society's toolkit for schools', which can be found at www.irms.org.uk

**7b.3 Biometric recognition systems**
In school we do not currently collect, store or use any form of biometric information.

If this changes in the future, staff, parents/carers and their children will be notified before any biometric recognition system is implemented or before any biometric data is collected. Furthermore, the school will also obtain written consent from each member of staff and at least one parent/carer of each child.

Where staff, parents/carers and their child/ren don't want to provide such data or use a biometric recognition system, they would have the right to choose not too and will be provided with an alternative means of accessing

the relevant services provided using such a system. Staff, parents/carers and their child/ren would also be able to withdraw consent, at any time, and, as a result we would make sure any relevant data already captured is deleted.

**CCTV**
In school we do not currently have CCTV cameras.

If this changes in the future, staff, parents/carers and their children will be notified before any CCTV cameras are installed, along with the safety reasons for this. We would also adhere to the ICO's code of practice for the use of CCTV equipment.

Whilst we do not need to ask an individuals' permission to use CCTV equipment, we would make it clear where individuals are being recorded. Security cameras would also be clearly visible and accompanied by prominent signs explaining that CCTV is in use.

## 8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:
- There is an issue with a pupil or parent/carer that puts the safety of our staff or themselves at risk.
- We need to liaise with other agencies, (we will seek consent as necessary before doing this)
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils. For example, IT companies. When doing this, we will:
  - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.
  - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement. This is to ensure the fair and lawful processing of any personal data we share.
  - Only share data that the supplier or contractor needs in order to carry out their service and only information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:
- The prevention or detection of crime and/or fraud.
- The apprehension or prosecution of offenders.
- The assessment or collection of tax owed to HMRC.
- In connection with legal proceedings.
- Where the disclosure is required to satisfy our safeguarding obligations.
- Research and statistical purposes as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

## 9. Subject access requests and other rights of individuals

If we process your data you have a number of rights as an individual which are summarised below.

### 9.1 Right to be informed
You have the right to be informed about the collection and use of your personal data. As a result we provide privacy information about the purposes for which we process your personal data, our retention periods for that personal data, and who it will be shared with. This will be provided to you at the time we collect it through our privacy notice which can be found in the appendix of this policy.

### 9.2 Subject access requests
Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:
- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purposes of the data processing.
- The categories of personal data concerned.
- Who the data has or will be shared with.
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.

- The source of the data, if not the individual.
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests should be submitted in writing, either by letter or email to the DPO. They should include:
- Name of individual.
- Correspondence address.
- Contact number and email address.
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the DPO.

**9.3 Children and subject access requests**
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

**9.4 Responding to subject access requests**
When responding to requests, we:
1. May ask the individual to provide 2 forms of identification.
2. May contact the individual via phone to confirm the request was made.
3. Will respond without delay and within 1 month of receipt of the request.
4. Will provide the information free of charge.
5. May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within 1 month and explain why the extension is necessary.

**N.B –** Please be aware that during closure periods we are unlikely to be able to deal with your request promptly so we ask that, wherever possible, you submit requests during term time.

We will not disclose information if it:
- Might cause serious harm to the physical or mental health of the pupil or another individual.
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.
- Is contained in adoption or parental order records.
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.
When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

**9.4 Other data protection rights of the individual**
In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it, individuals also have the right to:
- Withdraw their consent to processing at any time.
- Have inaccurate personal data rectified or completed if it is incomplete.
- Have personal data erased, (also known as the 'right to be forgotten').
- Request the restriction or suppression of your personal data in certain circumstances.
- Prevent use of their personal data for direct marketing.
- Challenge processing which has been justified on the basis of public interest.
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.
- Object to decisions based solely on automated decision making or profiling, (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress.
- Be notified of a data breach in certain circumstances.
- Make a complaint to the ICO.
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format, (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## 10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record, (which includes most information about a pupil) within 15 school days of receipt of a written request.

## 11. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. (See Appendix 5) We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:
- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns.
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

For more information see our:
- Safeguarding and Child Protection Policy
- E-safety Policy and Use of Mobile Phone's Policy
- Photo consent form
- Freedom of Information Policy
- Staff, governor and Volunteer Acceptable User Agreement

## 12. Data protection by design and default

Within the school we have put measures in place to show that we have integrated data protection into all of our data processing activities, including:
- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law.
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies, (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices.
- Regularly reviewing with members of staff information relating to data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 13. Data security and storage of records

Clarendon Primary School is committed to ensuring that the personal data we hold and process is kept secure at all times and that data protection is considered and integrated into our processing activities. We use a variety of technical and organisational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure, or unauthorised access.

These include:

- Only authorised personnel can access, alter, disclose or destroy personal data.
- Authorised personnel understand the limits of their authority and to whom they should escalate any issues relating to personal data.
- Appropriate backup systems are in place so that, if personal data is accidentally lost, altered or destroyed, it can be recovered.
- Access to premises or equipment given to anyone outside the school, (for example, for computer maintenance purposes) is strictly regulated and access to data limited.
- Staff receive training on data protection principles and their responsibilities as appropriate to their role, including highlighting the possibility that they may commit a criminal and/or disciplinary offence if they deliberately try to access or disclose information without authority.
- Strict guidelines on the appropriate use of computers to reduce the risk of the network being compromised.
- Regular review our physical security measures, such as ease of access to the premises through entrances and internal doors, alarm systems, lockable storage and security lighting.
- A process in place for the secure disposal of paper waste.
- Portable IT equipment is appropriately encrypted so that data contained on such devices is secure.
- Confidential paper files are not taken off site unless appropriate security measures have been implemented first.
- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use.
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards or left anywhere else where there is general access.
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.
- Third parties who process data on our behalf are compliant with data protection law.
- We have an appointed Data Protection Officer in place who monitors and reports on our accountability and governance measures.

## 14. Disposal of records

Personal information is kept and stored in accordance with a data retention schedule, the full version of which is available to view from www.irms.org.uk. (See appendix 8 for retention schedule details.) The retention schedule lays down the length of time which records need to be retained and the action which should be taken when it is of no further administrative use and follows all relevant legislation, which include the Data Protection Act 2018, the Freedom of Information Act 2000, the General Data Protection Regulation 2016 and the Education Act.

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.
For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

**School Closures**

In the event of the school closing, it is the responsibility of each Local Authority (LA) to manage the records of closed schools until they have reached the end of their administrative life and to arrange for their disposal when required.

In the event of the school subsequently becomes an Academy, the records relating to the pupils, who are transferring to the Academy, will be transferred. If the Academy is retaining the current buildings, then all records relating to the maintenance of the buildings will also be transferred. All other records become the responsibility of the Local Authority.

## 15. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches; however, in the event of a data breach taking place, we will report the circumstances to the Information Commissioner within 72 hours of becoming aware that it has occurred. We will also keep a register of data breaches that have occurred. If a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also inform those concerned directly and without undue delay. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a school laptop containing non-encrypted personal data about pupils.

## 16. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

## 17. Links with other policies

This data protection policy is linked to our:

- Freedom of information Policy
- Safeguarding and Child Protection Policy
- E-safety Policy
- Freedom of Information Policy
- Mobile Phone Policy
- Staff, governor and Volunteer Acceptable User Agreement
- Photo consent form
- Staff Code of Conduct and Staff handbook
- Clarendon Primary School & Nursery Workforce Privacy Notice (Appendix 2)
- Clarendon Primary School & Nursery Privacy Notice (Appendix 3)

## 18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing the effectiveness of this policy.

This policy will be reviewed **every 2 years** or when changes in legislation requires us to do so. It will then be agreed by the full governing body.

## 19. Policy review

Last reviewed: Summer Term 2020
Date for review: Summer Term 2022